Doing our best to achieve our best

Clarendon Primary School and Nursery
Data Protection Policy and Procedures

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 legal guidance and legislation. This includes the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018) and the Privacy & Electronic Communications (EC Directive) Regulations (PECR) 2003.

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 meets the current requirements of UK Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the EU GDPR, PECR 2003, UK GDPR and DPA 2018. It is also based on the information provided by the Article 29 Working Party.

Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to video surveillance, and the DBS Code of Practice in relation to handling sensitive information.

Furthermore, this policy complies with 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. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username etc

	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: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • 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. 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 United Kingdom. (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 Data Protection Law.

These are where:

- The individual (or their parent/carer, where appropriate), has given explicit consent.
- It is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment of a Data Controller or of a Data Subject.
- It is necessary to protect the vital interests of the Data Subject.
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.
- The Personal Data has manifestly been made public by the Data Subject.
- There is the establishment, exercise or defence of a legal claim.
- There are reasons of public interest in the area of public health.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

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 servces/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.

10. Artificial intelligence (AI) Artificial intelligence

AI tools are now widespread and easy to access. Staff, pupils and parents / carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The school recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, the school will treat this as a data breach, and will follow the personal data breach procedure outlined in this policy.

11. Transferring Data Internationally

We may send your information to other countries where we or a company we work with store information on computer servers based overseas; or when we need to communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk. Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

12. 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.

12.1 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.

12.2 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.

12.3 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.

12.4 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 United Kingdom.
- 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.

13. 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.

14. 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

15. 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.
- Periodic audits will be undertaken to monitor and review 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.

16. 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.

17. Disposal of records

Personal information is kept and stored in accordance with the IRMS data retention schedule, (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.

18. 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:

- Personal data being left unattended in a meeting room/staffroom/PPA room.
- Sending information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent.
- 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.

19. 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
- Mobile Phone Policy
- Staff, governor and Volunteer Acceptable User Agreement
- Photo consent form
- Staff Code of Conduct and Staff handbook
- Disaster Recovery/Business Continuity Plan
- 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: Autumn Term 2024
Date for review: Autumn Term 2026

Appendix 1:
Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people

- The DPO will alert the headteacher and the chair of governors.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage, (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

  - The DPO will document the decision, (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. As this information is likely to be of a sensitive nature all documented decisions will be stored on the school's computer 'S' drive in a folder entitled 'DPO data breaches'. (N.B – Access to this drive to restricted to key members of staff.)

  - Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
      - The categories and approximate number of individuals concerned.
      - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

  - If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

  - The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals. For example, the police, insurers, banks or credit card companies.

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again, (such as establishing more robust processes or providing further training for individuals)

- Records of all breaches will be stored on the school's computer 'S' drive in a folder entitled 'DPO data breaches'. (N.B – Access to this drive to restricted to key members of staff.)

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data, (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to recall it.*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.*

Other types of breach that you might want to consider could include:

- *Details of pupil premium interventions for named children being published on the school website.*
- *Non-anonymised pupil exam results or staff pay information being shared with governors.*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked.*
- *The school's cashless payment provider being hacked and parents' financial details stolen.*

Appendix 2:
Clarendon Primary School and Nursery
Workforce Privacy Notice

The purpose of this privacy notice is to explain to you the data we collect about you as part of your employment relationship, or other work engagement, with the school.

Name of data controller: Clarendon Primary School and Nursery
Knapp Road
Ashford
Middlesex
TW15 2HZ

Name of our data protection officer: Mrs Carol Foley

What information do we collect about our workforce and how?

The categories of school workforce information we collect, process, hold and share include, (but not restricted to):

- Personal information, (such as name, contact details for you and your emergency contacts, employee or teacher number, bank account and national insurance number)
- Information about your entitlement to work in the UK.
- Information about your remuneration, including payroll records, tax status information and entitlement to benefits such as pensions or insurance cover.
- Special categories of data, (including information about your ethnic origin, medical and health conditions, any recorded disability, nationality and country of birth)
- The terms and conditions of your employment and contract information, (such as start dates, hours worked, post, roles and salary information)
- Information about your marital status, next of kin, dependants and emergency contacts.
- Contact details and preference, (contact telephone numbers, email addresses, addresses)
- Details of trade union membership where provided by yourself or your trade union.
- Work attendance and absence information, (such as your work pattern history, number of absences and reasons)
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals as well as the reasons for the leave.
- Work performance and history, (such as appraisal reports and correspondence, information about any performance improvement plans and related correspondence, information about disciplinary or grievance matters, including any warnings issued to you)
- Information about your criminal record.
- Information from your application form and recruitment process, such as qualifications and employment history, (including start and end dates with previous employers and with the organisation) skills, experience, ongoing training data and, where relevant, subjects taught.
- Data from our IT systems which records your use of the internet and work email account. This is collected and managed on behalf of the school by the Future Digital service.
- Staff photos used on SIMS, the school website and for Identification Lanyards.

We collect information from you both prior to and during your employment from a range of sources, including your application form, correspondence with you, forms you complete prior to and during employment, from interviews, appraisals and other meetings.

Why we collect and process this information

Personal data processed for the performance of a contract or to comply with legal obligations
We process this information because the processing is necessary for us to enter into an employment, (or other work-related) contract with you and for the subsequent performance of that contract. For example, to ensure you are paid and receive your entitlements to benefits, such as annual leave. We also need to process this information to ensure that we are complying with our legal obligations, such as ensuring that we deduct tax correctly, and to defend legal claims. Furthermore, this information will support effective performance management and appraisal of staff.

Equal opportunities monitoring
We process special category data, such as information about your ethnic origin or health, as part of our equal opportunities monitoring process, because the school has a legitimate interest in processing this data. Where we process information for the purposes of equal opportunities monitoring, this information is collected only with the express consent of employees. Consent may be withdrawn by an employee at any time. We process data in this category in reliance on the condition that processing is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment.

Other processing of special category data and criminal records data
We also process special category data, such as information about health, racial or ethnic origin, to comply with our legal obligations, (such as conducting 'right to work' checks, ascertaining fitness to work, meeting our obligations under health and safety legislation and the Equality Act 2010) or because processing is necessary for the performance of the contract, (such as administering sick pay).

We process criminal records data to help facilitate the safer recruitment of staff, (as part of our safeguarding obligations towards pupils) and to comply with our legal obligations to ensure the suitability of employees and other workers to work with children and young people.

We process data in this category in reliance on the condition that processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law in connection with employment.

Personal data processed for the purposes of the legitimate interests of the employer

We use other school workforce data to manage the day-to-day operation of the school, where processing is necessary for the purposes of the legitimate interests of the employer. In relying on legitimate interests, we first consider the necessity of processing the data when balanced against the interests, rights and freedoms of the individual. These legitimate interests include to:

- Manage and inform recruitment and retention processes and respond to reference requests.
- Inform the development of recruitment and retention policies.
- Keep records of employee performance and work history, including training and appraisal records, to ensure acceptable standards of conduct are maintained and to manage training and career progression.
- Manage absence effectively.
- Manage day-to-day HR administration.
- Enable the development of a comprehensive picture of the workforce and how it is deployed. (This includes the completion of statutory data returns to the Local Authority and Department for Education)
- Manage payment of additional expenses to staff via BACS using the schools FMS system.
- Fulfil our Safeguarding policies are effectively implemented.
- Support the implementation and monitoring of our policies and procedures.
- Comply with the law regarding data sharing.
- Allow for better financial modelling, administration and planning.

We do not make employment decisions based on automated decision-making.

If we wish to process your personal data for a new purpose we will inform you of any additional processing.

Automated-decision making

We do not make employment decisions based on automated decision-making.

Using personal data for new purposes

If we wish to process your personal data for a new purpose we will inform you of any additional processing.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

We will endeavour to complete data updates on an annual basis.

Storing this information

We hold school workforce data securely in your personnel file, in electronic records within our HR system and also in other IT systems, including email.

Your information is stored in accordance with a data retention schedule.

In summary, we retain most records relating to your employment on your personnel file for six years after employment has ended.

Evidence of your right to work in the UK is retained on your personnel file for two years after employment has ended, in accordance with Home Office recommendations.

Allegations of a child protection nature remain on file until normal retirement age, or 10 years from the date of the allegation, if longer, in accordance with statutory guidance. (This information is shared with the Local Authority Designated Officer (LADO) in line with Policy and Practice.)

Identity documents obtained for the purposes of undertaking a Disclosure and Barring Service check are only retained until the results of the check have been received.

Who we share this information with and why

Your information will be shared with appropriate school staff, with an HR or recruitment responsibility, and managers within your area of work or department.

We do not share information about workforce members with anyone without consent unless the law and school policies allow us to do so.

Beyond the school, we share your information when necessary with the local authority, in order to comply with legal obligations and statutory guidance regarding the safeguarding of children and young people.

We also share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment of educational attainment. See the section below on ‘Department for Education data collection requirements’ for further detail.

Other third parties

We will share your data with certain third parties to fulfil legal requirements, obtain or provide necessary information or because the third party processes data on our behalf. These third parties include:

- Family or representatives authorised by you – such as in the event of an emergency.
- Educators and examining bodies – such as ensuring we adhere to examining regulations to guarantee the validity of examinations.
- Your previous employers in order to undertake pre-employment checks.
- The Disclosure and Barring Service in order to undertake pre-employment checks and follow-up checks during employment.
- Ofsted.
- Payroll.
- Suppliers and consultants that provide us with a service, such as occupational health, HR or legal services.
- Trade unions or any other representative acting on your behalf.
- Central and local government – such as workforce analysis.
- Health authorities and Occupational Health and employee support schemes – to ensure the wellbeing of our staff body in accordance with our responsibilities as employer.
- Health and social welfare organisations – to ensure the wellbeing of our staff body in accordance with our responsibilities as employer.
- Charities and voluntary organisations to assist in the provision of extra-curricular enrichment activities e.g. PTA led events or supplying references to charities our staff wish to work in tandem with.
- Police forces, courts, tribunals – to ensure we act in the public interest or fulfil a legal obligation.

When we appoint third parties to process data on our behalf, the third party is also required to process the data lawfully and fairly and in a manner that ensures appropriate security of the data, using appropriate technical or organisational measures to protect against unauthorised or unlawful processing and accidental loss.

We do not generally transfer your data to countries outside the European Economic Area; however where we do, we will do so in accordance with data protection law.

Department for Education data collection requirements

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our school employees with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

The workforce data that we lawfully share with the DfE through data collections:

- Informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce.
- Links to school funding and expenditure.
- Supports 'longer term' research and monitoring of educational policy.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data.
- The purpose for which it is required.
- The level and sensitivity of data requested; and
- The arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms & conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

How to find out what personal information the DfE holds about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- If they are processing your personal data.
- For a description of the data they hold about you.
- The reasons they're holding it and any recipient it may be disclosed to.
- For a copy of your personal data and any details of its source.

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:
https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data and your rights as a data subject

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our data protection officer, (details at the beginning of this document).

You also have the right:

- To have your personal data rectified, if it is inaccurate or incomplete.
- To request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- To restrict our processing of your personal data, (i.e. permitting its storage but no further processing).
- To object to direct marketing, (including profiling) and processing for the purposes of scientific/historical research and statistics.
- Not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

How to access personal information we hold

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- Give you a copy of the information we hold in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request for this please contact our Data Protection Officer, (details shown at the start of this document).

Further information

If you would like to discuss anything in this privacy notice, please contact our data protection officer, (details at the beginning of this document).

Appendix 3:
Clarendon Primary School and Nursery
Privacy Notice

How we use student and parent information

Under General Data Protection Regulations, (GDPR) we are obliged to inform you of the information we hold on your child/ren, what we use it for, who we share it with and for how long we keep it. This privacy notice aims to provide you with this information. If it, or any information linked to it is unclear, please contact the School Office or the School's Data Protection Officer. Contact details for both are available in Section 11 at the end of this privacy notice.

We, Clarendon Primary School and Nursery, Knapp Road, Ashford, Middlesex, TW15 2HZ are the Data Controller for the purposes of data protection law. We are registered with the Information Commissioner's Office and our registration number is Z8998857.

As a public body we have appointed a Data Protection Officer (DPO) Mrs Carol Foley. Our DPO can be contacted at the School address or by email dataprotection@clarendon.surrey.sch.uk.

The categories of pupil and parent information that we collect, hold and share include but are not limited to:

- Personal information, (such as name, unique pupil number, parents' national insurance number)
- Contact details and contact preference order, (contact telephone numbers, email addresses, home addresses)
- Characteristics, (such as ethnicity, religion, language, country of birth and free school meal eligibility)
- Safeguarding information, (such as court orders and professional involvement)
- Special educational needs information, (including information relating to the specific needs of a child and any EHCP or EHA requests/documentation)
- Information relating to Looked After and previously Looked After Children.
- Relevant medical information and administration, (such as doctors' information, child health, dental health, allergies, medication, medical conditions, any disabilities, dietary requirements and information relating to lunch time arrangements)
- Attendance information, (such as sessions attended, number of absences, reasons for absence and any previous schools attended)
- Assessment and attainment information, (such as Early Years Foundation Stage Profile information, Key Stage 1, Key Stage 2 and phonics results, internal assessment data for all year groups as well as any other relevant assessment results)
- Behavioural information, (such as exclusions and any relevant alternative provision put in place)
- Personal information required for the appropriate delivery of offsite trips; these include residential visits.
- Photographs for internal safeguarding and security purposes, school newsletters, school data system, media and promotional purposes. (NB. separate consent is also obtained where required)
- Payment details, (collected and processed by WisePay on behalf of the school)
- Information relating to meetings with parents, (such as parents' evenings and other relevant meetings undertaken with staff at the school or other professionals working on behalf of the school)
- Information relating to meetings with children, (such as concerns raised regarding events in school or incidents with other children)

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we collect and use pupil and parent information

We collect and use pupil information, for the following purposes:

- To support pupil learning.
- To monitor and report on pupil attainment progress.
- To provide appropriate pastoral and medical care.
- For safeguarding and pupil welfare purposes.
- For research purposes.
- To inform you about events and other things happening in school.

- To assess the quality of our services.
- To keep children safe, (such as details of any food allergies as well as emergency contact details)
- For the purposes of child protection.
- Where applicable, to ensure the safe and effective delivery of sessions provided by either the school's nursery or after school club.
- To meet the statutory duties placed upon us for DfE data collections.
- To ensure any activities occurring offsite are delivered in a safe and efficient manner.
- To comply with the law regarding data sharing.

The lawful basis on which we use this information

Our lawful basis for collecting and processing pupil information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- Data subject gives consent for one or more specific purposes.
- Processing is necessary to comply with the legal obligations of the controller.
- Processing is necessary to protect the vital interests of the data subject.
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller, (the provision of education).

Our lawful basis for collecting and processing pupil information is also further defined under Article 9, in that some of the information we process is deemed to be classified as sensitive or special information and the following sub-paragraphs in the GDPR apply:

- The data subject has given explicit consent.
- It is necessary to fulfil the obligations of the data controller or of the data subject.
- It is necessary to protect the vital interests of the data subject.
- Processing is carried out in the course of our legitimate activities.
- Reasons of public interest in the area of public health.
- It is in the public interest.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and will explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

An example of how we use the information you provide is for the submission of the school census returns, including a set of named pupil records, which is a statutory requirement on schools under Section 537A of the Education Act 1996.

The provision of statutory information for e.g. school census and data returns:

- Means that schools do not need to obtain parental or pupil consent to the provision of information.
- Ensures schools are protected from any legal challenge that they are breaching a duty of confidence to students.
- Helps to ensure that returns are completed by schools.

Collecting pupil information

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

We collect pupil information via:

- Information provided by parents, e.g. when completing registration forms at your child's point of entry to the school or when your child takes part in a specific activity, (this information is updated annually to ensure it remains accurate).
- Information provided by parents when requesting a place in either the school's nursery, breakfast or after school clubs.
- Information received via a CTF, (Common Transfer File) provided by your child's previous school.
- Other information provided by your child's previous school.

- Information provided by other external agencies, (these include, but are not limited to, health, children's services, speech and language, occupational therapy, educational psychology and CAMHS).

How we store pupil data

We hold pupil data securely for a set amount of time whilst the child remains at Clarendon Primary School & Nursery and in some instances for a set period of time after leaving, for example when a pupil does not transfer immediately to another school. Clarendon Primary School & Nursery retains information in accordance with the Information Records Management Society guidance on data retention schedules. (Further information can be found in the 'Information Management Toolkit for Schools' at www.irms.org.uk)

We have data protection policies and procedures in place which are regularly reviewed.

Who we share pupil information with

We routinely share pupil information with appropriate third parties. These include:

- The local authority in order to meet legal obligations with regards to sharing certain information, such as safeguarding concerns and exclusions.
- Department for Education.
- The pupil's family and representatives.
- Educators and the STA (Standards Testing Agency)
- Ofsted.
- Suppliers and service providers to enable them to provide the service we have contracted them for, e.g. Target Tracker, SIMS, WisePay, Teachers2Parents and carefully selected providers who offer a range of supporting educational software used by the school to support each child's education.
- Financial organisations.
- Central and local government.
- Auditors.
- Survey and research organisations.
- Health authorities.
- Health and social welfare organisations.
- School nursing team.
- Professional advisers and consultants.
- Charities and voluntary organisations.
- Police forces, courts, tribunals.
- Professional bodies.
- Schools that the pupils attend after leaving us.

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.

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the DfE either directly or via the local authority:

- We are required to share information about pupils with the local authority (LA) and the Department for Education under section 3 of The Education (Information about Individual Students) (England) Regulations 2013.
- We are also required to share information about pupils with the Department for Education under regulation 5 of The Education (Information about Individual Students) (England) Regulations 2013.

This data sharing underpins a range of functions which include school funding and educational attainment policy and monitoring.

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools or see Appendix 4 'How Government uses your Data'.

National Pupil Database

As identified above, we are required by law to provide information about pupils to the Department for Education as part of statutory data collections such as the school census. Some of this information is then stored in the National Pupil Database, (NPD) which is owned and managed by the Department for Education and provides evidence on school performance to inform research.

The law that allows this is the Education (Information about Individual Pupils) (England) Regulations 2013. The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards. The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

Decisions on whether the DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data.
- the purpose for which it is required.
- the level and sensitivity of data requested.
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Requesting access to your personal data

Under data protection legislation parents and pupils have the right to request access to information about them that we hold through a Subject Access Request. To make a request for your personal information or to be given access to your child's educational record, contact the Data Protection Officer whose details can be found in Section 11.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it.
- Tell you why we are holding and processing it and how long we will keep it for.
- Explain where we got it from; if not from you or your child.
- Tell you who it has or will be shared with.
- Give you a copy of the information in an intelligible form.

In certain circumstances, individuals also have the right for their personal information to be transmitted electronically to another organisation.

If you would like to make a request please contact our Data Protection Officer using the contact details provided in Section 11.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.
- A right to seek redress, either through the ICO, or through the courts.

Making a complaint

If you have a concern or wish to make a complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact the DPO:

Mrs Carol Foley
Clarendon Primary School & Nursery
Knapp Road
Ashford
Middlesex
TW15 2HZ

Email: dataprotection@clarendon.surrey.sch.uk
Tel: 01784 253379

Appendix 4

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

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

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

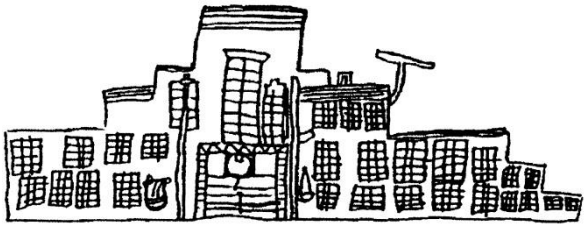
For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website:
https://www.gov.uk/government/publications/dfe-external-data-shares

To contact DfE: https://www.gov.uk/contact-dfe

Appendix 5

Clarendon Primary School and Nursery

SURREY COUNTY COUNCIL



Headteacher
Mr William Neale

'Doing our best to achieve our best'

Knapp Road
Ashford
Middlesex
TW15 2HZ
Tel: 01784 253379
Fax: 01784 421745
clarendonschool@googlemail.com

PHOTOGRAPHIC IMAGES OF CHILDREN – CONSENT FORM

Child's name: _____ Child's class:_____

To ensure that we comply with Data Protection Law, we need your permission to photograph or make any recording of your child during their time at Clarendon. Please tick and initial to confirm your consent or otherwise for each sub-section.

What	Where	Yes	No
1. Use of your child's image or name	In school *e.g. on display boards, in class and around the school*		
2. Your child's name and/or image *NB. They will be unidentifiable by full name and photograph combined unless agreed in advance with an adult who holds parental responsibility*	School publications *e.g School Newsletter (please note, this is also uploaded as a PDF onto the school website)*		
3. Your child's name or image *NB. They will be unidentifiable by full name unless agreed in advance with an adult who holds parental responsibility*	School on-line publications *e.g. school website and the school's online prospectus*		
4. Your child being photographed, filmed or published on an external multi or social media page. *News media may publish pictures along with the child's full name, but the school will seek an undertaking that a child's name will not be used if their image is put on the newspaper's own website.*	External press/media *e.g. newspapers, television images and/or social media pages. (For example, used by a charity working with the school)*		

NB The school uses a range of external software applications for educational purposes. For example, TT Rockstars, Class DoJo, MyMaths, Purple Mash etc. These programmes ensure that children's names and passwords are stored on a secured database.

Declaration: I have read and understood the consent asked of me above, including my child's use of a range of external software applications used by the school. My decision on whether to give consent will remain valid for my child's time at Clarendon unless I notify the school in writing informing them that I wish to withdraw my consent. This can be done at any time. NB. Parents will also be given the opportunity to review this information if reqd.

I promise that if I, or members of my family, take photographs or video recordings at a school event, these will be kept for family use only and will not be uploaded to social media.

Parent's Name: _____

Parent's Signature: _____

Date: _____

Appendix 6
Clarendon Primary School and Nursery School
Privacy Notice for Supply, Consultants and Contractors

Name of data controller: Clarendon Primary School and Nursery
Knapp Road
Ashford
Middlesex
TW15 2HZ

Name of our data protection officer: Mrs Carol Foley

Under General Data Protection Regulations, (GDPR) we are obliged to inform you of the information we hold on you, including what we use it for, who we share it with and for how long we keep it. This privacy notice, (also known as a 'fair processing notice') aims to provide you with this information. If any information is unclear, please contact the Data Controller. (Contact details are available above.)

The categories of information that we collect, hold and share include, but are not limited to:

- Personal information, (such as name, address, national insurance number).
- Contact details and preference, (contact telephone numbers, email addresses, addresses).
- Characteristics, (such as ethnicity, religion, language, nationality, country of birth)
- The terms and conditions of your deployment with us including contractual terms.
- Details of your qualifications, skills, experience and employment history where required.
- Payment details where applicable.
- Information about your emergency contacts or associated procedure.
- Information about your entitlement to work in the UK.
- Information about your criminal record.
- Details of your schedule, (days of work and working hours) and attendance at work.
- Information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments and fulfil its duty of care, (including the use of Occupational Health Services)
- Photographs, (for internal safeguarding & security purposes, school newsletters, media and promotional purposes).

We may also hold personal data about you from third parties, such as references supplied by former employers or service users, information provided during the completion of our pre-deployment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

Why we collect and use this information

The purpose of collecting and processing this data is to help us run the school efficiently, including to:

- Fulfil our legal obligations in relation to Keeping Children Safe in Education.
- Develop all aspects of the school operationally.
- Inform our operational procedures.
- Allow better financial modelling, administration and planning.
- Provide references where requested.
- Allow us to fulfil or legal and contractual obligations.
- To assess the quality of our services.
- To comply with the law regarding data

The lawful basis on which we use this information

Our lawful basis for collecting and processing staff information is defined under Article 6, and the following subparagraphs in the GDPR apply:

(a) Data subject gives consent for one or more specific purposes.
(c) Processing is necessary to comply with the legal obligations of the controller.

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following subparagraphs in the GDPR apply:

(a) The data subject has given explicit consent.
(b) It is necessary to fulfil the obligations of controller or of data subject.
(d) Processing is carried out by a foundation or not-for-profit organisation, (this includes religious, political or philosophical organisations and trade unions)

Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

Collecting Your Information
Whilst the majority of information you provide to us is mandatory or related to our mutual contractual obligation, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Storing your data
We create and maintain filing system related to these individuals. The information contained in these files is kept secure and is only used for purposes directly relevant to your deployment with us. Once your deployment with us has ended, we will retain this file and delete the information in it in accordance with the retention schedule outlined in our data protection policy.

We have data protection policies and procedures in place, which are regularly reviewed. (A copy of this policy is available on our school website.)

Who we share information with
We routinely share supply, contractor and consultant information with appropriate third parties, including:

- The local authority – to meet our legal obligations to share certain information with them, such as safeguarding concerns
- Your agency or employer regarding the service provided.
- Suppliers and service providers – to enable them to provide the service we have contracted them for.
- Our auditors, to ensure our compliance with our legal obligations.
- Security organisations – to create a secure school environment.
- Professional advisers and consultants – used to help us to develop our service.
- Police forces, courts, tribunals.
- Future employers – references.

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.

Why we share your information
We do not share information about you with anyone without consent unless the law and our policies allow us to do so. The majority of the information shared will be to manage the mutual contractual obligations in place around the services being provided.

Data collection requirements
Our data collection requirements all relate to the our legal and contractual obligations, for example contract clauses or the statutory 'Keeping Children Safe in Education Guidance'.

Requesting access to your personal data and your Data Protection Rights
Under data protection legislation, you have the right to request access to information about you that we hold, through a Subject Access Request. If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you or your child.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- Give you a copy of the information in an intelligible form.

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our Data Controller. (Contact details outlined above.)

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.
- Claim compensation for damages caused by a breach of the Data Protection regulations.

Complaints
We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance by contacting our data controller. (Contact details outlined above.)

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF 11.

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data controller. (Contact details outlined above.)

Appendix 7
Letter templates

DATA PROTECTION ACT 2018 – SUBJECT ACCESS REQUEST

Dear _____

Thank you for your request which we received on_____. Your request falls under the Data Protection Act 2018 as your request is for personal information concerning your child.

We do take the handling of personal data seriously and we ask you to please provide two proofs of ID such as a copy of your passport/birth certificate and a copy of proof address such as a utility bill. This is to ensure that we are sending personal data to the right individual.

In order for us to process your request efficiently, it would be most helpful if you can specify the date range that you require information for and any particular information that you require. As you can understand there is a large amount of information held and we wish to ensure that you are supplied with the relevant information.

On receipt of the above ID we will process your request within the one month statutory reply period.

Yours Sincerely,

Dear

RE: YOUR REQUEST UNDER THE DATA PROTECTION ACT 2018

Thank you for your subject access request dated XXXX. Subject access requests are for personal data about the requester that is focused on the requester. It is for data/information and not the documents in which the data/information is found.

You have been quite specific in your request, which was for the following information held by the school:

STATE REQUEST

We searched our relevant systems to locate data within the scope of your request. The data retrieved was reviewed by the Senior Management to ensure it was your personal data.

- I confirm that we are processing the personal data specified in your request.

I enclose with this letter a copy of the document/s specified in your request.

We have redacted any reference to third parties where applicable and where we owe a duty of confidentiality.

I hope that the information attached satisfies your request.

If you are unhappy with the contents of the information provided, its accuracy or retention, or with the handling of your request, then you should raise this by writing to the Chair of Governors.

If, following this, you are not satisfied by the School's response to your complaint, you have the right to apply to the Information Commissioner for a decision. The Information Commissioner will normally expect you to have exhausted our complaints procedure. The Information Commissioner can be contacted at the Cheshire address below.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

We supply this information based on your original request. Please do not hesitate to contact me at the above address, should you have any queries regarding the information enclosed.

Yours sincerely,

Headteacher

Data Retention Schedule 8

Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[1]
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
	Inspection Copies[2]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Please note that all information about the retention of records concerning the recruitment of Head Teachers can be found in the Human Resources section below.

1.2 Head Teacher and Senior Management Team					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
1.3.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL

1.3 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.4.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

2.2 Operational Staff Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning[6] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	written warning – level 1			Date of warning + 6 months	
	written warning – level 2			Date of warning + 12 months	
	final warning			Date of warning + 18 months	
	case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

2.5 Payroll and Pensions					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

3. Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals.

3.1 Risk Management and Insurance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	

5.1 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
	This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

7. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.2 Walking Bus					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

7.3 Family Liaison Officers and Home School Liaison Assistants					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

8. Central Government and Local Authority

This section covers records created in the course of interaction between the school and the local authority.

8.1 Local Authority					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL

8.2 Central Government					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL