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's 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 ICT 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, Nursery and Family Centre
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, Nursery and Family Centre
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, the full version of which is available to view from www.irms.org.uk.

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, Nursery and Family Centre
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, Nursery and Family Centre , 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. I will get the Family Centre ICO registration number

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 2a '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.

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