CASTLE PARK SCHOOL
Learning For Life

DATA PROTECTION POLICY

Reviewed on: **14th May 2018**

Signed: *Wendy Gibson* **(Chair)**

CASTLE PARK SCHOOL
Learning for Life

Appendix A - Access to Personal Data Request

Appendix B - Privacy Notice – Pupils in Schools and Early Years Settings

CASTLE PARK SCHOOL
Learning for Life

DATA PROTECTION POLICY

1. Rationale

Castle Park School (hereinafter referred to as 'the School') is committed to a policy of protecting the rights and privacy of individuals, including students, staff and others, in accordance with the Data Protection Act, 1998 (DPA).

The School needs to process certain information about its staff, students and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- the recruitment and payment of staff
- the administration of programmes of study
- the recording of a student's progress
- agreeing awards
- collecting monies
- complying with legal obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the Data Protection Act, 1998, the School must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. Associated School Policies

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Online Safety Policy and procedures
- CCTV Policy and Procedures
- Health and Safety Policy
- Procedures for Using Pupils' Images
- Whole School Behaviour Policy
- Staff Code of Conduct (see Staff Handbook)
- Data Processing Procedures (from 25th May 2018)

3. Compliance

This policy applies to all governors and trustees, staff and students of the School. Any breach of this policy, or of the Act itself will be considered an offence and the School's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with the School, and who have access to personal information, will be expected to read and comply with this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the DPA and other relevant legislation.

The Information Commissioner's Office (ICO) https://ico.org.uk/ gives further detailed guidance and the School undertakes to adopt and comply with ICO guidance.

4. The Data Protection Act, 1998

This piece of legislation came into force on 1 March 2000 (updated 25.5.18). The DPA regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request' (sample held at Appendix A). Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs and video; CCTV images), and may include facts or opinions about a person.

The DPA also sets out specific rights for School students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Student Information) (England) Regulations 2000.' For more detailed information on these Regulations see the Data Protection Guide on the ICO website.

5. Responsibilities Under the DPA and Registration

The School will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.

The Headteacher of the School is responsible for all day-to-day data protection matters, and she will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the School.

The School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

The Headteacher is also responsible for ensuring that the School's notification is kept accurate. Details of the School's notification can be found on the ICO website.

Compliance with the legislation is the responsibility of all members of the School who process personal information.

Individuals who provide personal data to the School are responsible for ensuring that the information is accurate and up-to-date.

6. Definitions

Data Controller:	Any individual or organisation who controls personal data, in this instance the School.
Personal Data:	Data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
Sensitive Personal Data:	Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual orientation and criminal activities.
Relevant Filing System:	Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records.
Data Subject:	An individual who is the subject of the personal data, for example, employees, pupils, parents, etc.
Processing:	Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.
***Accessible Records*:**	Any records which are kept by the Organisation as part of a statutory duty, e.g. pupil records, SEND records, child protection records.
Parent:	Has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

7. Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, the School undertakes to:

7.1 Process personal data fairly and lawfully

The School will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

7.2 Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose

The School will ensure that the reason for which it collected the data originally is the only reason for which it processes the data, unless the individual is informed of any additional processing before it takes place.

7.3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed

The School will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals, they will be destroyed immediately.

7.4 Keep personal data accurate and, where necessary, up to date

The School will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the School if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the School to ensure that any notification regarding the change is noted and acted upon.

7.5 Only keep personal data for as long as is necessary

The School undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means the School will undertake a regular review of the information held and implement a data cleansing process when, pupils or a member of staff leaves the School for example.

The School will dispose of any personal data in a way that protects the rights and privacy of the individual concerned. See also Section 16.

7.6 Process personal data in accordance with the rights of the data subject under the legislation

Individuals have various rights under the legislation including:

- a right to be told the nature of the information the School holds and any parties to whom this may be disclosed;
- a right to prevent processing likely to cause damage or distress;
- a right to prevent processing for purposes of direct marketing;
- a right to be informed about the mechanics of any automated decision making process that will significantly affect them;
- a right not to have significant decisions that will affect them taken solely by automated process;
- a right to sue for compensation if they suffer damage by any contravention of the legislation;
- a right to take action to rectify, block, erase, or destroy inaccurate data;
- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened;

The School will only process personal data in accordance with individuals' rights.

7.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

The School will ensure that all personal data is accessible only to those who have a valid reason for using it.

The School will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access;
- keeping all personal data in a lockable room with key-controlled access;
- password protecting or encrypting personal data held electronically;
- archiving personal data which is then kept securely (lockable cabinet);
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not be visible except to authorised staff.

In addition, the School will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal, or if that is not possible, destroyed physically.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in such circumstances additional care must be taken regarding the security of the data.

7.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The School will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so the School will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If the School collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

8. Consent as a Basis for Processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when Schools are processing any sensitive data, as defined by the legislation.

The School understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

The School will ensure that any forms used to gather data on an individual will contain a statement (Privacy Notice – formerly known as Fair Processing Notice) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

The School will ensure that if the individual does not give their consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

8.1 Fair Processing

Under the "Fair Processing" requirements in the Data Protection Act, the School will inform staff and separately, parents/carers of all pupils, of the data they hold on the staff member or pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This fair processing notice, now known as a Privacy Notice will be passed to staff when they join the School and parents/carers when the child joins the school. The School's Privacy Notices can be found at Appendix B.

9. Subject Access Rights (SARS)

The Data Protection Act extends to all data subjects the right of access to their own personal data. In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Although this is most unlikely at this school, where a request for subject access is received from a pupil, the School's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

9.1 Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form (see Appendix A), available from the School Office. Completed forms should be submitted to the Headteacher. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester *(if different)*, the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

10. Authorised Disclosures

The School will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the School to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the School.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example, to the school's IT technician during maintenance of the computer system. In such circumstances the IT technician would be required to comply with the school's Data Protection policy and their own company's privacy terms and conditions, in which they ensure not to disclose the data outside the School. Officers and IT personnel writing on behalf of the

LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the School by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working with the School who need to know the information in order to do their work.

- Legal Disclosure

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the School, provided that the purpose of that information has been registered.

10.1 Illegal Disclosure

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

11. Publication of School Information

The School occasionally (e.g.for an educational visit) publishes various documents which will include some personal data, e.g.

- Staff/parent contact telephone numbers
- staff details
- class/group list

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted to internal staff access only. Therefore, it is school policy to offer an opportunity to opt-out of the publication of such documents when collecting the information.

Staff records appertaining to individual staff will remain of a confidential nature between the Headteacher and the member of staff and, where appropriate, the school's administrators.

11.1 Email

It is the policy of the School to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the School's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the School may be accessed by someone other than the recipient for system management and security purposes.

11.2 CCTV

There are CCTV systems operating within the School for the purpose of protecting school members and property. The School will only process any personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

For detailed guidance on CCTV refer to the ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 which can be found at https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf and the School CCTV Procedures.

Images/Photographs

Information regarding our policy for the use of pupils' images and Parental Consent forms can be found in the following documents:

- KCP Use of Digital Images Policy
- Online Safety Policy

- Parental Consent Form For Use of Photographs and Images on the Website
- Child Protection Policy

12. Data Integrity

The School undertakes to ensure data integrity by the following methods:

12.1 Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances, their computer record will be updated as soon as is practicable. A printout of their data record (Data Collection Sheet) will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

12.2 Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The admission form pack is reviewed annually by the office, in collaboration with the Headteacher, and any information deemed unnecessary is removed.

12.3 Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the office staff to ensure that obsolete data is properly erased. See also Section 16.

13. Data and Computer Security

The School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

13.1 Physical Security

Appropriate building security measures are in place, such as alarms, deadlocks, CCTV, anti-climb measures, outdoor sensor lighting, lockable gates, magnetic locks on all external doors with door fobs. Only authorised persons are allowed in the IT suite or photocopying/printer areas. Visitors to the School are required to sign in and out, to wear identification badges whilst in the School and are, where appropriate, accompanied.

13.2 Logical Security

- Security software is installed on all computers containing personal data.
- The School will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.
- All users have secure user names and passwords. which must be changed regularly. User names and passwords are only shared between authorised users. (See Online Safety Policy)
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

- Personal data can only be stored on school equipment (this includes computers and portable storage media) *where allowed*. Private equipment (i.e. owned by the users) can only be used with appropriate permissions and data protection e.g. encrypted pen drives.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - the data must be encrypted or password protected;
  - the device must be password protected or encrypted e.g. school encrypted pen drive
  - the device must offer approved virus and malware checking software;
  - the data must be securely deleted from the device, in line with School policy (below) once it has been transferred or its use is complete.
- The School has clear policy and procedures for the automatic backing up, accessing and restoring all data held on School systems, including off-site backups. The IT system is physically backed up every day, with a copy being kept off site.
- Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign their contract of employment which includes a confidentiality agreement. Data Protection obligations and requirements are part of the staff induction process upon appointment. Staff are given updates as necessary. Computer printouts, as well as source documents, are shredded before disposal or put into the school's confidential sacks for authorised disposal.

Further information can be found in the school's Online Safety Policy.

Overall security policy for data is determined by the Headteacher/Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the School should in the first instance be referred to the Headteacher.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

14. Secure transfer of data and access out of School

The School recognises that personal data may be accessed by users out of School, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the School or authorised premises without permission and unless the media is encrypted or password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of School.
- When data is required by an authorised user from outside the School premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS), teacher's server or office server.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (NB. to carry encrypted material is illegal in some countries)

15. Disposal of Data

The School will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded or placed in the school's confidential sack.

16. Training & Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

Induction training for new staff;

- Staff meetings/briefings/Inset;
- Day to day support and guidance from the Team Leaders/Headteacher.

17. Enquiries

Information about the School's Data Protection Policy is available from the school office. General information about the Data Protection Act can be obtained from the Information Commissioners Office https://ico.org.uk/.

A copy of this policy will be available to all employees and covered in new staff Induction Training. It will be reviewed at least biennially, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

APPENDIX A

ACCESS TO PERSONAL DATA REQUEST

(Subject Access Request – SARS)

DATA PROTECTION ACT 1998 (Section 7)

Enquirer's Surname		**Enquirer's Forenames**	
Enquirer's Address			
Enquirer's Postcode:			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			**YES / NO**
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			**YES / NO**
If YES,			
Name of child or children about whose personal data records you are enquiring:			
Description of Concern / Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

APPENDIX A

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED) _____

Dated _____

CASTLE PARK SCHOOL

Learning For Life

PRIVACY NOTICE
FOR
PUPIL INFORMATION

Review Date ……

Signed …….. (Chair of Governors)

Next Review ……

Privacy Notice (How we use Pupil Information)

The categories of pupil information that we collect, hold and share include:

- Personal information such as name, unique pupil number and address;
- Secondary personal information e.g. parent/carer name and contact details, doctor and dentist contact details
- Characteristics such as gender, ethnicity, language, religion, nationality, country of birth and free school meal eligibility, traveller/refugee status, images (photographic and video);
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Assessment information;
- Relevant medical information, dietary information;
- Special educational needs and disabilities information;
- Exclusions/Behavioural information;
- School history
- Support information such as child protection status, Child Looked After, adopted, service child status, pastoral information.

Why we collect and use this information

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing;
- to allow for better financial modelling and planning;
- to enable accurate ethnicity and disability monitoring.

The lawful basis on which we use this information

We collect and use pupil information under General Data Protection Act (GDPR) Article 6.1 (c), necessary for compliance with a legal obligation and GDPR Article 9.2 (c) necessary to protect the vital interests of a data subject, or another individual, where the data subject is physically or legally incapable of consenting

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, 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 pupil information to us or if you have a choice in this.

Storing pupil data

We securely hold pupil data for a period when the child is enrolled at the school and for a period of between one and three years where a pupil has left the school, depending on the nature of the data. We store and maintain pupil data for a variety of purposes. For example in relation to: SATS results, attendance, safeguarding, child protection, standards, Health and Safety and SEND, retaining information for up to the child's date of birth plus 25 years max. For a more detailed breakdown of the retention of pupil data, please see our Retention of Pupil Records Policy, which is available at the school office. Our Data Protection Policy is available either through the office or on the policies page of the school website at www.castleparkschool.org.uk

Who we share pupil information with

We routinely share pupil information with:

- schools to which pupils transfer after leaving Castle Park School;
- the local authority;
- the Department for Education (DfE);
- National Health Service
- ScholarPack (Management Information System)
- LunchShop (School Lunch Management System)
- School Money (Payment Management System)
- External Residential and Educational Visit Providers
- External agencies e.g. Educational Welfare Officer, Educational Psychologists, School Counsellors, Music Teachers, Itek Computer Systems

This list is not exhaustive and will be added to as and when necessary.

Why we 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.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

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)

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.
We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.
The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether 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; and
- 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-how-we-collect-and-share-research-data
For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received
To contact DfE: https://www.gov.uk/contact-dfe

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. To make a request for your personal information, or be given access to your child's educational record, please contact, via a letter, the school office.
You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, blocked, erased or destroyed 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
- object to processing of personal data that is likely to cause, or is causing, damage or distress
- claim compensation for damages caused by a breach of the Data Protection regulations

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

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the school office on 01539 790440.

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated in **November 2018.**

Contact

If you would like to discuss anything in this privacy notice, please contact between the school office between the hours of 8.30am – 3.45pm;

Telephone no. 01539 790440