

GDPR and Data Protection Policy

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

The school as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the School and all staff comply with the legislation.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information¹. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)

¹ GDPR Article 4 Definitions

4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA (European Economic Area) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards².

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party³
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the

² These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

³ The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited⁴ unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
 - (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
 - (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
 - (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
 - (d) the 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
 - (e) the processing relates to personal data which are manifestly made public by the data subject
 - (f) the processing is necessary for the establishment, exercise or defence of legal claims
 - (g) the processing is necessary for reasons of substantial public interest
 - (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
 - (i) the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

⁴ GDPR, Article 9

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

Automated Decision Making

Where the school carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The School must as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request the school to reconsider or take a new decision. If such a request is received staff must contact the DPO as the school must reply within 21 days.

Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the School's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

Documentation and records

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

As part of the School's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- DPIAs and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The School should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notice

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The School will issue a minimum of two privacy notices, one for pupil information, and one for workforce information see Appendix 1 and 2.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The School maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed (*see the relevant privacy notice*)
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request (*see Appendix 1 - Procedure for Access to Personal Information*)
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information

Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:

http://www.kelsi.org.uk/_data/assets/word_doc/0012/60213/InformationManagementToolkitforSchoolsv4-2.docx

Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Training

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (<https://ico.org.uk/>) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Privacy Notice for Workforce

This notice explains what personal data (information) we hold about you, how we collect, how we use and may share information about you. We are required to give you this information under data protection law.

Who are we?

Portal House collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the General Data Protection Regulation which applies across the European Union (including in the United Kingdom) and we are responsible as ‘controller’ of that personal information for the purposes of those laws. Our Data Protection Officer is SPS DPO Services.

The personal information we collect and use

Information collected by us

In the course of employing staff in our school we collect the following personal information when you provide it to us:

- Personal information (such as name, address, contact details, employee or teacher number, national insurance number)
- Characteristics (such as gender, age, ethnic group)
- Contract information (such as start dates, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Relevant medical information

How we use your personal information

We use your personal information to:

- Enable individuals to be paid
- Support pension payments and calculations
- Enable sickness monitoring
- Enable leave payments (such as sick pay and maternity leave)
- Develop a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Inform financial audits of the school
- Fulfil our duty of care towards our staff
- Inform national workforce policy monitoring and development

How long your personal data will be kept

We will hold your personal information for 6 years in line with KCC’s personnel retention record keeping guidelines.

Reasons we can collect and use your personal information

We rely on having a legitimate reason as your employer to collect and use your personal information, and to comply with our statutory obligations, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

We are required to share information about our workforce members under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Who we share your personal information with

- Department for Education (DfE)
- Kent County Council Management Information.
- Kent County Council Schools Financial Services
- Commissioned providers of personnel and payroll services (Capita, SPS)

We will share personal information with law enforcement or other authorities if required by applicable law.

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

The DfE 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 DfE 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 school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Your Rights

Under the GDPR you have rights which you can exercise free of charge which allow you to:

- Know what we are doing with your information and why we are doing it
- Ask to see what information we hold about you (Subject Access Requests)
- Ask us to correct any mistakes in the information we hold about you
- Object to direct marketing
- Make a complaint to the Information Commissioners Office
- Withdraw consent (if applicable)

Depending on our reason for using your information you may also be entitled to:

- Ask us to delete information we hold about you
- Have your information transferred electronically to yourself or to another organisation
- Object to decisions being made that significantly affect you
- Object to how we are using your information
- Stop us using your information in certain ways

We will always seek to comply with your request however we may be required to hold or use your information to comply with legal duties. Please note: your request may delay or prevent us delivering a service to you.

For further information about your rights, including the circumstances in which they apply, see the guidance from the UK Information Commissioners Office (ICO) on individuals' rights under the General Data Protection Regulation.

If you would like to exercise a right, please contact SPS DPO Services.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Who to Contact and Where to go for Further Information

Please contact Mrs Rose Bradley to exercise any of your rights, or if you have a complaint about why your information has been collected, how it has been used or how long we have kept it for.

If you would like to get a copy of the information about you that KCC shares with the DfE or how they use your information, please contact the Information Resilience and Transparency Team at data.protection@kent.gov.uk.

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/concerns> or telephone 03031 231113.

For further information visit <https://www.kent.gov.uk/about-the-council/about-the-website/privacy-statement>

For further information about how the Department for Education uses your information:

To find out more about the staff information we share with the DfE, for the purpose of data collections, go to <https://www.gov.uk/education/school-workforce-censuses>

For more information about the DfE'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>



Privacy Notice for pupils

1. Privacy notice for Parent/Carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about pupils.

We, Portal House School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is the SPS Data Protection Officer Services.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Name
- Contact details, contact preferences, date of birth, identification documents
- Parental, sibling and extended family details
- Children who are adopted from care, looked after children, under special guardianship
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, language, eligibility for free school meals, Pupil Premium or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs of your child
- Carefully chosen and vetted educational apps
- CCTV images

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 use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care

- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

In order to meet statutory requirements around appropriate education provision and to fulfil safeguarding requirements, we share information about school history and the latest known pupil and parent address and contact details in the event of a Child Missing Education, or becoming Electively Home Educated. This information also supports the in-year admissions process.

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

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 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.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

Children's records are stored securely in paper files and on the school's secure server.

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We will adhere to the Information Management Toolkit for Schools Document.

Data sharing

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

Where it is legally required, or necessary (and it complies with the General Data Protection Regulation, otherwise known as the GDPR) we may share personal information about pupils with:

- Our local authority (e.g. admissions)
- The Department for Education (e.g. attainment)
- The pupil's family and representatives (e.g. attendance)
- Educators and examining bodies (e.g. SATS test papers)
- Our regulators Ofsted, DFE and the ESFA (e.g. pupil data)

- Suppliers and service providers (e.g. sports coaches)
- Central and local government (e.g. attainment)
- Health authorities (e.g. immunisations)
- Health and social welfare organisations (e.g. social services)
- Professional advisers, bodies and consultants (e.g. Educational psychologist)
- Police forces, courts, tribunals (in relation to safeguarding)
- Collaborating schools for moderating purposes

National Pupil Database

We are required 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 and provides evidence on school performance to inform research.

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.

For more information, see the Department's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) with any further questions about the NPD.

Transferring data internationally

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.

Parents and pupils' rights regarding personal data

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

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 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.

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact Mrs Bradley Headteacher.

If you require access to the above, please apply in writing, citing your reasons to the Headteacher.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Headteacher.

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 the school in the first instance.

To make a complaint, please contact our Headteacher.

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

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Headteacher in the first instance.

Mrs R Bradley headteacher@portal-house.kent.sch.uk

Data Protection Officer: SPS DPO Services

Email: sps-dpo-services@isystemsintegration.com

Address: SPS SPO Services, iSystems Integration, Devonshire House, 29-31 Elmfield Road, Bromley, Kent BR1 1LT

This notice is based on the [Department for Education's model privacy notice](#) for the school workforce, amended to reflect the way we use data in this school.

