Data Protection Policy

Last reviewed: May 2023
Next Review: May 2024

Oaklands School is committed to protecting the rights and freedoms of data subjects and to the safe and secure processing of their data, in accordance with the General Data Protection Regulation (GDPR). The GDPR replaces the EU Data Protection Directive of 1995 and superseded the laws of Member States that were developed in compliance with the Data Protection Directive 95/46/EC. It took effect in UK law with the coming into force of the Data Protection Act 2018. The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. All those who work in the UK now need to comply with the Data Protection Act 2018 (DPA 2018).

We hold personal data about our employees, staff, students, suppliers and other individuals for a variety of educational and business purposes.
This policy sets out how we seek to protect personal data and ensure that our employees understand the rules governing their use of the Personal Data to which they have access in the course of their work.

In particular, this policy requires the data controller and senior leaders to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Oaklands School's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all our employees to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

Definitions

For the purposes of this policy, the following words and phrases are defined thus:

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll, educational and general business purposes Organisational purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring business policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments - Monitoring staff conduct, disciplinary matters - Marketing our school - Improving services

Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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.
Special categories [of personal data]	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	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; where the purposes and means of such processing are determined by law.
Data processor	A natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.
Processing [of data]	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the United Kingdom Information Commissioner's Office. They can be contacted at the below address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, UK
GDPR	The General Data Protection Regulations
Data Protection Act 2018	The UK law through which the GDPR came into force in the UK.
EU	The European Union
EEA	The European Economic Area
ICO	The UK Information Commissioner's Office

Policy Objectives

The school as the Data Controller will comply with its obligations under the UK DPA 2018. 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.

Policy Scope

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. 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.

Our Data Protection Officer

Our Data Protection Officer is The DPO Centre. If you have any questions about this policy, or concerns regarding how the school collects or processes data, please contact them. They can be contacted via email at advice@dpocentre.com, via telephone at **0203 797 6340**, or via physical mail at **50 Liverpool Street, London, EC2M 7PY**.

The Principles of the GDPR

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

1. **Lawfulness, fairness and transparency** - Personal data must be processed lawfully, fairly and in a transparent manner

2. **Purpose limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes/

3. **Data minimisation** - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed ()

4. **Accuracy** - 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.

5. **Storage limitation** - 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.

6. **Integrity and confidentiality** - 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.

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA 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 safeguards.

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 bases 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 school 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 school or by a third party
- 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 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 prohibited[1] unless a lawful special condition for processing is identified.

[1] GDPR, Article 9

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:
  - the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
  - the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
  - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
  - 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
  - the processing relates to personal data which are manifestly made public by the data subject
  - the processing is necessary for the establishment, exercise or defence of legal claims
  - the processing is necessary for reasons of substantial public interest
  - 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
  - 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.

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.

Data relating to criminal offences

Any criminal record checks (Disclosure and Barring Service checks, Barred List checks, List 99 checks) are justified by law[2]. Criminal record checks cannot be undertaken based solely on the consent of the subject. The school must not and does not keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

Criminal record checks will be carried out by the school for all staff and volunteers.

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

[2] In most cases the requirement will come from the Safeguarding Vulnerable Groups Act 2006 (Schedule 4 Part 1)

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.

As of the last review of this policy, the school does not carry out any form of automated decision making or profiling.

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, and these will be reviewed in line with any statutory or contractual changes. Copies of these are Appendices A and B to this policy.

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 and retention schedules

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 [Appendix C to this policy] 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.
- 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 unencrypted devices, or on personal devices that are used for work purposes.

Information Security

See the Information Security Policy for full details of the measures used to secure data and systems.

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.

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, malware 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.

Subject Access Requests

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information, which means the information, which should be provided in a privacy notice.

Processing Subject Access Requests

- We must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

- If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.

- We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

- Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

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.

Appendix A: Privacy Notice (staff, volunteers and Governors)

This notice is to make clear how and why Oaklands School collects personal information about you and what we do with this data. Oaklands School is the data controller of the personal information you provide us. The school determines the purposes for which any personal data relating to staff is to be processed.

Why do we collect and use your information?

We collect and use personal data in order to meet the legal requirements and legitimate interests set out in the General Data Protection Regulation (GDPR) and UK law, including those in relation to the following:

- Article 6(1)(e) – public task, data processing which is necessary to allow the school to function, and Article 9(2)(e) – data processed with the explicit consent of an individual
- The Education Act 1996

We also use the data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid

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

- Personal information (such as name, employee or teacher number, national insurance number)
- Special categories of data including characteristics information 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) and training information
- Relevant medical information

For Governors, we use the data to:

- Enable the development of a comprehensive picture of governance and how it is deployed
- Enable appropriate checks to be completed
- Enable individuals to be kept informed of governance training and relevant information

Collecting school workforce information

Whilst the majority of staff 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 school workforce information to us or if you have a choice in this.

Storing school workforce information

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally intended.

Personal data relating to the school workforce is stored in line with the school's Data Protection Policy and Retention Schedule

Who do we share school workforce information with?

We routinely share school workforce information with:

- our local authority, the London Borough of Hounslow
- the Department for Education (DfE)
- the school's Payroll Provider
- Occupational Health

We routinely share school governance information with:

- our local authority, the London Borough of Hounslow
- the Department for Education (DfE) through Get Information About Schools (GIAS)
- other Governors on the Governing Body

Why we share school workforce information

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

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

We 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 educational attainment.

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

All members of staff, volunteers and Governors are required to have an enhanced criminal records disclosure from the Disclosure and Barring Service, including Barred List checks. Information may be shared to facilitate this.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools 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 census submissions because it is a statutory return under Sections 113 and 114 of the Education Act 2005.

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 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

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

Requesting access to your personal data

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, or be given access to your child's educational record, contact the school office (office@oaklands.uk.net ; 020 8560 3569)

Our Data Protection Officer is The DPO Centre. If you have any questions about this policy, or concerns regarding how the school collects or processes data, please contact them. They can be contacted via email at **advice@dpocentre.com**, via telephone at **0203 797 6340**, or via physical mail at **50 Liverpool Street, London, EC2M 7PY**.

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; and
- 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, you should raise your concern with us in the first instance.

Alternatively, you can contact the Information Commissioner's Office at **https://ico.org.uk/concerns/**

Appendix B: Privacy Notice (students and parents)

This notice is to make clear how and why Oaklands School collects personal information about you and what we do with this data. Oaklands School is the data controller of the personal information you provide us. The school determines the purposes for which any personal data relating to pupils and their families is to be processed.

Why do we collect and use your information?

Oaklands School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, the Local Authority (LA) and/or the Department for Education (DfE). We collect and use personal data in order to meet the legal requirements and legitimate interests set out in the General Data Protection Regulation (GDPR) and UK law, including those in relation to the following:

- Article 6(1)(e) – public task, data processing which is necessary to allow the school to function, and Article 9(2)(e) – data processed with the explicit consent of an individual
- The Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- To safeguard pupils

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

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such national curriculum assessment results / levels)
- Behaviour information
- Relevant medical information (such as allergies)
- Information relating to SEND

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

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally intended.

Personal data relating to pupils at Oaklands School and their families is stored in line with the school's Data Protection Policy and Retention Schedule.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority, the London Borough of Hounslow
- the Department for Education (DfE)
- Exam boards or accreditation boards

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies require or 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 pupil information we share with the department, for the purpose of data collections, go to **https://www.gov.uk/education/data-collection-and-censuses-for-schools**

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
- 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 the DfE: **https://www.gov.uk/contact-dfe**

Appendix C: Retention Schedule

Data item	Retention period	Notes
Student data		
Admissions files	1 year after student leaves school	
Admissions appeals	5 years after event	
Attainment	5 years after student leaves school	
Attendance	1 year after student leaves school	
Behaviour		
Free school meals eligibility	7 years after student leaves school	Impacts finances – hence 7 year retention period for audit reasons
Trips and activities (basic information)	Destroy once trip complete	
Medical information and administration (*not* incidents or any safeguarding data)	1 year after student leaves school	
Safeguarding information	35 years after student leaves school	
Special Educational Needs files, reviews and individual education plans		
Other student data unspecified	1 year after student leaves school	
Financial data		
Payroll and wage records	7 years after end of tax year they relate to	
Pension records	12 years	
Parental (maternity/paternity) leave records	3 years after end of relevant tax year	
Statutory Sick Pay records		
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	7 years from end of relevant scheme year	
Current bank details of employees	No longer than necessary for payroll purposes	
Other school financial records unspecified	7 years after end of tax year they relate to	
General administration		
Visitors' signing in details	2 years after event	

Emails not covered by another category	3 years after receipt	
CCTV footage not covered elsewhere (e.g. not relating to a Safeguarding incident)	1 year after recording	
Governors and Governing Body meetings		
Minutes of meetings	Permanently	
Governors' personal contact details, training logs and pecuniary interest forms	1 year after end of term of office	
Meeting administration (agenda, action plans)	3 years after date of meeting	
Employment, recruitment and Human Resources		
Job applications and interview records of unsuccessful candidates	6 months after notifying unsuccessful candidates, unless consent received to keep details on file	
Job applications and interview records of successful candidates	7 years after employment ceases	
Written particulars of employment, contracts of employment and changes to terms and conditions		
Disciplinary and training records		
Right to work documentation including identification documents and immigration checks	2 years after employment ceases	
DBS checks and disclosures	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.	
Emergency contact details	Immediately on employment ceasing	
Annual leave records	7 years after end of relevant tax year	
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer)	

Trade union agreements	10 years after ceasing effect	
Professional development plans	5 years after ceasing effect	
Records relating to hours worked and payments made to temporary, casual or agency workers	3 years after end of relevant tax year	
Health and Safety (H & S)		
H & S consultations	Permanently	
Risk assessments	3 years after ceasing effect	
Any reportable accident, death or injury in connection with work	12 years after report date	
Other accident reporting	Adults – 6 years from the date of the incident Children – until child is aged 25	
Fire alarm test books	5 years after last entry	
Records in the scope of the Control of Substances Hazardous to Health (COSHH) Regulations	40 years from creation date	
Records of tests/examinations of control systems and protection equipment in the scope of the COSHH Regulations	5 years from record date	