OAKS PARK HIGH SCHOOL

DATA PROTECTION POLICY

Approved by:	**Date:** May 2018
Next review due by:	May 2020

Contents

01. Aims

Our School aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998 and the General Data Protection Regulation 2018.

This policy applies to all data, regardless of whether it is in paper or electronic format.

02. Legal framework

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

In addition, this policy complies with the General Data Protection Regulation, May 2018.

This policy has due regard to legislation, including, but not limited to the following:

- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy will be implemented in conjunction with the following other School policies:

- E-safety Policy
- Student Privacy Notice
- Staff Privacy Notice

03. Definitions

Applicable Data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which

are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Definitions Table

Term	Definition
Personal data	Relates to a living individual who can be identified from the data or other information held/likely to be held by the data controller (even where they are not named e.g. from a reference number), including opinions about the individual or what is intended for them. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.
Sensitive personal data	Data such as: ● Contact details ● Racial or ethnic origin ● Political opinions ● Religious beliefs, or beliefs of a similar nature ● Where a person is a member of a trade union ● Physical and mental health ● Sexual orientation ● Whether a person has committed, or is alleged to have committed, an offence ● Criminal convictions The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
Processing	Obtaining, recording, holding information, or carrying out operations on data including: • Organisation, adaptation or alteration of data • Retrieval, consultation or use of data • Disclosure of data by transmission, dissemination or other ways of making available • Alignment, combination, blocking, erasure or destruction of data

Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Inaccurate data	Incorrect or misleading data.
Recipient	Anyone to whom data are disclosed unless disclosure is being made as part of a legal inquiry.
Third party	Any person other than the data subject, the data controller, any data processor or other person authorised to process data .

04. Data protection and GDPR principles

The **Data Protection Act** 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

Under the **General Data Protection Regulations** 2018, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

05. Roles and responsibilities

The **governing board** has overall responsibility for ensuring that the School complies with its obligations and all current legislations.

OPHS is the **data controller** for the purposes of the act and therefore have overall responsibility for compliance with the DPA and GDPR.

OPHS have delegated responsibility to the **Headteacher** in each School for ensuring compliance with this policy within the day-to-day activities of the School.

OPHS has appointed a **Data Protection Officer** (DPO). The DPO is responsible and required to perform several tasks under GDPR. They include the following:

- Inform and advise the organisation and its employees of their data protection obligations under the GDPR.
- Monitor the organisation's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes.
- Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting.

- Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this this and all our policies.

Staff must also inform the School of any changes to their personal data, to make sure this is accurate and up to date.

06. Accountability

We do implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

We provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The School implements measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Regularly management and improvement of our security features.

Data protection impact assessments will be used, where appropriate.

07. Privacy/fair processing notice

A privacy notice is a statement that describes how this organisation, uses, retains and discloses personal information. Different Organisations sometimes use different terms and it can be referred to as a privacy statement, a fair processing notice or a privacy policy.

To ensure that we process your personal data fairly and lawfully we are required to inform you:

- What Information we collect, hold and share.
- Why we collect and use this information
- The lawful basis on which we use this information.
- Who we share this information with.
- Why we share this information.
- Our Data collection requirements.
- How you can access this data and your rights.

This information also explains what rights you have to control how we use your information. The law determines how organisations can use personal information. The key laws are: the Data Protection Act 1998 (DPA), the Human Rights Act 1998 (HRA), the General Data Protection Regulation 2018 (GDPR), relevant educational legislation, and the common law duty of confidentiality.

7.1 Students Privacy notice

Please refer to the *Students Privacy policy*

7.2 Staff Privacy Notice

Please refer to the *Staff Privacy policy*

08. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

The consent of the data subject has been obtained.

Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:

    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

09. Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The School ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

10. The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the School will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - o Withdraw consent at any time.
    - o Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the
  significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

11. The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The School will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the School may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the School holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.

12. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the School will inform them of the rectification where possible.

Where appropriate, the School will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the School will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The School has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information of the School
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the School will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

14. The right to restrict processing

Individuals have the right to block or suppress the School's processing of personal data.

In the event that processing is restricted, the School will store the personal data, but not further

process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The School will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the School has verified the accuracy of the data
- Where an individual has objected to the processing and the School is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the School no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the School will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The School will inform individuals when a restriction on processing has been lifted.

15. **The right to data portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. The School will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The School is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the School will consider whether providing the information would prejudice the rights of any other individual.

The School will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the time frame can be

extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the School will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

16. The right to object

The School will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The School will stop processing the individual's personal data unless the processing is for the

  establishment, exercise or defence of legal claims, or, where the School can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The School will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The School cannot refuse an individual's objection regarding data that is being processed for

  direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the School is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the School will offer a method for individuals to object online.

17. Privacy by design and privacy impact assessments

The School will act in accordance with the GDPR by adopting a privacy by design approach and

implementing technical and organisational measures which demonstrate how the School has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the School's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the School to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Timu School School's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The School will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the School will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

18. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Principal will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the School becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the School will notify those concerned directly.

A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the School, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure itself. to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

19. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.
Where possible, the School enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for School purposes.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the School premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the School containing sensitive information are supervised at all times.

The physical security of the School's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

The School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information

The School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

The School will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the School website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The School notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for six months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access.

The School will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the School wishes to use images/video footage of pupils in a publication, such as the School website, prospectus, or recordings of School plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

22. Data retention

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the School may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Subject access requests

Under the Data Protection Act 1998 and the General Data Protection Regulation 2018 (GDPR) individuals have the right to request access to information any organisation holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter or email to the Data Protection Officer at DPO@oakspark.redbridge.sch.uk.

Requests should be done through this form as a template or guidance:

https://docs.google.com/document/d/15qYJrVfo8egV39hAwAPlLdo2NmWiwUiYi_zH9In7EXc/edit

The School will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

25. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our School may not be granted without the express permission of the pupil.

26. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staff room tables or pinned to noticeboards where there is general access

- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access School computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software/hardware is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for School-owned equipment

27. Disposal of records

The School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

The School will always choose a qualified source for disposal of IT assets and collections.

28. Training

Our staff and governors are provided with Data Protection and GDPR training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation or the School's processes make it necessary.

We have also implemented a yearly programme to train staff, SLT and Governors in all areas of Data Protection and GDPR. This training programme will be consistent, ongoing and relevant.

29. The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018.

We will review working practices when this new legislation takes effect and provide training to members of staff and governors where appropriate.

30. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

At every review, the policy will be shared with the governing board.