GDPR - **General Data Protection Regulation Policy**

Headteacher	Ms. Caroline Rowlandson (CR)	**Data Protection Officer (DPO)**	Mr. Gary Hipple Gary.Hipple@richmondandwandsworth.gov.uk
IT Manager	Mr. Chivna Tseayo (ICT)	**Data Manager**	Ms. Tara Abidi (TCA)
Current Policy review date	30th September 2024	**Next Review Date**	30th September 2025
Policy Reviewed by whom	Chivna Tseayo, Tara Abidi & Caroline Rowlandson	**School Address**	Oak Lodge School, 101 Nightingale Lane, Balham, LONDON, SW12 8NA

Introduction

Oak Lodge School is committed to protecting and respecting the privacy of personal data in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines the way in which Oak Lodge School collects, uses, processes and stores personal data and the rights of individuals regarding their data.

Scope

This GDPR policy applies to everyone including all current, past and prospective pupils, parents, guardians, employees, contractors and volunteers whose personal data is collected, processed or stored by Oak Lodge School. All staff working within the School must be compliant with the GDPR policies and abide by the Data Protection Act at all times. Within this document you will find the outlines and descriptions of the varying processes and procedures that require adhering to.

GDPR - **General Data Protection Regulation Policy**

The Guiding Principles of GDPR

Lawfulness, Transparency & Fairness:	Accurately and lawfully processing data with a clear and plain language.
Purpose Limitation:	Having permission and a legitimate purpose to be processing any data
Data Minimisation:	The set guidelines per organization as to how long the data is held for.
Accuracy:	Recording all data according to what has been provided as accurate as possible to avoid any further implications of wrongful use. If the data is inaccurate it will need to be rectified or erased without delay.
Storage Limitation:	Personal data is securely stored ensuring no loss or unauthorized use.
Confidentiality & Integrity:	Ensuring that all data is appropriately and securely stored and protected at all times.

GDPR - **General Data Protection Regulation Policy**

Definitions

Personal Data:	Any information relating to the identity of an individual is considered personal data.
What Constitutes Personal Data:	Home address, email address, date of birth, bank details, medical information and sexuality.
Processing:	Any operation performed on personal data including collection, storage, use, disclosure and deletion.
Data Subject:	An Individual and their personal data.
Data Controller:	The entity that determines the purposes and means of processing personal data.
Data Processor:	The entity that processes personal data on behalf of the Data Controller.

GDPR - **General Data Protection Regulation Policy**

Data Collection

Oak Lodge School collects and processes personal data for the following purposes:

Educational Purposes	To provide education and related services.
Administrative Purposes	To manage Oak Lodge's operations including admissions, attendance and assessment.
Communication:	To communicate with pupils, parents & guardians about school activities and any events updates.
Safety & Welfare:	To ensure the safety and well-being of pupils and staff.
Legal Obligations:	To comply with statutory and regulatory requirements

GDPR - **General Data Protection Regulation Policy**

Types of Data Collected

Types of personal data collected by Oak Lodge School may include the following:

Pupils	Full name, date of birth, contact details, health information, school records which include attendance data & behaviour.
Parents & Guardians	Full name, contact details, relationship to the pupil and payment information.
Staff & Contractors	Full name, contact details, employment records, payment & salary information, qualifications and background checks.

GDPR - **General Data Protection Regulation Policy**

Legal Basis Processing

Oak Lodge School processes personal data based on one or more of the following legal bases:

Consent:	Where explicit consent has been obtained from the data subject.
Contractual Necessity :	Where processing is necessary for the performance of a contract.
Legal Obligation:	Where processing is required by law.
Legitimate Interests:	Where processing is necessary for the legitimate interests pursued by the school, provided these interests are not overridden by the data subjects' rights.

GDPR - **General Data Protection Regulation Policy**

Data Sharing and Disclosure

Oak Lodge School will only share personal data with third parties when necessary and in accordance with GDPR. This may include:

Education Authorities & Regulatory Bodies:	For compliance with legal obligations.
Service Providers :	For the provision of services such as IT support, payment processing and educational tools.
Examination Bodies:	For the delivery of examinations and results certificates.
Health & Social Services:	For safeguarding and welfare purposes.
Law Enforcement Agencies:	Where require by law.

Special Category Personal Data

Oak Lodge School may need to share data in the event of an emergency, incident or accident. These may include details of an individual's medical condition being shared with medical services, the police or social services.

GDPR - **General Data Protection Regulation Policy**

Data Security

Oak Lodge School implements appropriate technical and organisational measures to protect personal data against unauthorised access, loss, or destruction. These measures include:

Encryption:	Protecting data in transit and at rest
Access Controls:	Limiting access to personal data to authorised personnel only.
Data Minimisation:	Collecting only the data necessary for the specific use and purpose.
Security Measures Availability:	The data remains accessible and usable. For instance, if personal data is accidentally lost, altered or destroyed you will be able to recover it and prevent any harm or distress to the individuals involved.
Network Protection:	Protection from cyber-attacks or data breaches.

Sending emails containing person data externally can be hazardous to any organization if the bulk of the email is not encrypted or secure enough. The potential risk could result in hackers accessing the systems and the huge amounts of data passing through the systems potential resulting in a School Data breach. Hackers can capture any data that has not been password protected or encrypted.

GDPR - **General Data Protection Regulation Policy**

Data Retention

Oak Lodge School will retain personal data only for as long as necessary to fulfil the purposes for which it was collected as required by law. Once the data is no longer needed, it will be securely deleted following the Oak Lodge School's data retention policy.

Data Subject Rights

Under GDPR, data subjects have the following rights regarding their personal data:

Right to Access:	To obtain a copy of their personal data held by the school.
Right to Rectification:	To request correction of inaccurate or incomplete data.
Right to Erasure:	To request deletion of their personal data where there is no legal basis for it retention.
Right to Restrict Processing:	To request that processing their data is restricted in certain circumstances.
Right to Data Portability:	To request the transfer of their data to another organization.
Right to Object:	To object to the processing of their data in certain circumstances.

GDPR - **General Data Protection Regulation Policy**

Right to Withdraw Consent:	To withdraw consent at any time where processing is based on consent.

Data Breach Response
In the event of a data breach, Oak Lodge School will promptly assess the risk to data subjects and if necessary, notify the relevant supervisory authority the ICO and DPO within 72 hours. Where the breach is likely to result high risk data release of the rights and freedoms of individuals and the affected data subjects will also be informed. A data breach becomes an incident which requires a quick process to resolve it from escalating too much larger proportions.

Data Protection Officer (DPO)
Oak Lodge School has appointed a Data Protection Officer to oversee compliance with GDPR and to act as a first point of contact for data subjects should the school ever be impacted by data breaches or threats. The DPO has the overall accountability and responsibility for compliance to the Data Protection Procedures within the School and Local Authority.

Information Security
Information Security is sometimes considered as Cybersecurity. Both security measures look at the data held is a digital format or online and they do overlap. The GDPR and Data Protection act have worked extremely closely with the NCSC to work on an overall approach to the security principle to secure data from becoming accidentally or deliberately compromised. Information security also covers physical and organisational security measures where data is related.

GDPR - **General Data Protection Regulation Policy**

How to Keep Data Safe (Work & Personal)

All Data is sensitive information and needs to be treated responsibly by the individuals within an organisation and yourself otherwise the School could be liable of non-prevention of the rules and regulations of GDPR if any of these documents were to go missing, be lost, stolen or be involved in a Data Breach.

Secure Units	All Hard copies of documents containing sensitive pupil/staff data MUST be stored in a lockable cupboard or drawer.
Clear Desks	Do not keep any paperwork on your desk when unattended with visible staff/pupil data on show.
Lock Your Computer	When you leave your desk you MUST at all times Lock your Computer Screen.
Digital Data	All digital data requires to be saved into the correct places such as SharePoint, Shared Drives or with Encryption.
Data Saved in Unauthorised Places – High Risk	Staff who create and edit database spreadsheets for work that save -

Contd.	- them onto desktops affect the School retention periods of Data and are a high risk as these would not be logged, due to this there would be no security around their presence.
Passwords	Never share your passwords with any other individuals whether it is regarding a work account or a personal account. Make all password complex and different for each account. Also never write them down and store then in a password protector app.
Accounts Compromised	In this Modern society we all have to be wary of issues like these. If you receive any notifications that your devices, emails or passwords have been compromised – it is vital that you change these passwords immediately to avoid your work/personal data being distributed on the Dark Web.

Two-factor authenticator (2FA)	Set these on various website access. A lot of organisations use these now as an added data security feature
Software/ Network	Keep all software up to date to protect you from viruses and hacking. Use only secure networks to work online.
Security Tools	Use security tools like firewalls, anti-virus software and VPNs
Be aware of Suspicious emails	Never click on suspicious links. Check the authenticity before responding to dubious emails.
Traveling with Data	Back up your data in two places before you leave. Make sure your software is updated. Keep your devices with you at all times. Secure devices enabling 2-factor authenticator to block unauthorized access in a case of lost or stolen.

GDPR - **General Data Protection Regulation Policy**

Acronyms

GDPR	General Data Protection Regulation
DPO	Data Protection Officer
DDPO	Deputy Data Protection Officer
ICO	Information Commission Officer
CPD	Continuing Professional Development
FOI	Freedom of Information Log
Data Subject	The Individual & their data
NCSC	National Cyber Security Centre
Cybersecurity	The protection of your networks and information systems from attack
2FA	Two-Factor Authenticator
CR	Caroline Rowlandson (Headteacher)
TCA	Tara Abidi (Data Manager)

GDPR - **General Data Protection Regulation Policy**

GDPR & Data Protection Training

All staff must complete and pass the online CPD course via The Key Platform for GDPR. This ensures that all staff are aware of their own individual liberty and accountability across the school and within their own personal lives to keep their own personal data secure. These assessments are recorded against your HR records and will need to be taken every 2 years.
Https://cpd.thekeysupport.com/statutory-elearning/data-protection-and-the-uk-gdpr-for-school-staff/

Additional Information

More information can be located on the Wandsworth Portal -
https://s4s.wandsworth.gov.uk/Page/14035