inspirans flammas
posteritatis

ROSEMEAD
PREPARATORY
SCHOOL & NURSERY
DULWICH

P14 - DATA PROTECTION/GDPR POLICY

(INCLUDING EYFS)

The School is registered under the Data Protection Act 2018.

Background

Data protection is an important legal compliance issue for Rosemead. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notice). The School, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

The law changed on 25 May 2018, with the implementation of the General Data Protection Regulation (GDPR) and a new Data Protection Act 2018 (DPA 2018) was also passed to deal with certain issues left for national law. The DPA 2018 included specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

About this Policy

Everyone has rights with regard to the way in which their personal data is handled. During the course of the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.
Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Any breach of this policy may result in disciplinary action.
This policy sets out the basis on which the School will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

General Statement of the School's Duties
The School is required to process relevant personal data regarding workers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Data Protection Officer
The School has appointed Graeme McCafferty, Acting Head, as the Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 2018. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

The Principles
Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the Data Protection Act 1998. These provide that personal data must be: -

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Personal Data
Personal data covers information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, pupils and their parents, suppliers and marketing and business contacts. It includes expressions of opinion about the individual, any indication of someone else's intentions towards the individual, information necessary for employment such as the worker's name and address and details for payment of salary.

Processing of Personal Data
The School's policy is to process personal data in accordance with the applicable data protection laws as set out above. All staff have a personal responsibility for the practical application of this policy.

Staff should generally not process personal data unless:
- The individual whose details are being processed has consented to this;
- The processing is necessary to perform the School's legal obligations or exercise legal rights, or
- The processing is otherwise in the School's legitimate interests and does not unduly prejudice the individual's privacy.

When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the DPC.

Sensitive Personal Data
The School may, from time to time, be required to process sensitive personal data regarding a worker. Where sensitive personal data is processed by the School, the explicit consent of the worker will generally be required in writing.
The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

Processing of Credit Card Data
The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Bursar.

Accuracy, adequacy, relevance and proportionality
Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.
Individuals may ask the School to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the DPO.
Staff must ensure that personal data held by the School relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the DPO so the School's records can be updated.

Rights of Individuals
Workers have the right of access to information held by the School, subject to the provisions of the Data Protection Act 1998. Any worker wishing to access their personal data should put their request in writing to the DPO. Employees who receive a written request for personal data should forward it to the DPO immediately.
The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 30 days. The School may charge £10 for the provision of the requested personal data, as permitted by law. The information will be imparted to the worker as soon as is reasonably possible after it has come to the School's attention. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.
Staff should not send direct marketing material to someone electronically (e.g. by email) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the DPO about any such request. Staff should contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Exemptions
Certain data is exempted from the provisions of the Data Protection Act which includes the following:-

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPO.

Accuracy
The School will endeavour to ensure that all personal data held in relation to workers is accurate and kept up to date. Workers must notify the DPO of any changes to information held about them. A worker has the right to request that inaccurate information about them is erased.

Timely Processing
The School will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

Enforcement
If a worker believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the worker should utilise the School grievance procedure and should also notify the DPO.

Data Security
The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to both staff and pupils. As such, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headteacher. Where a worker is permitted to take data offsite it will need to be encrypted. As an added safeguard during lockdown, all remote data access is via secure GoogleDrive access.

P14 – Data Protection & GDPR

Author/s:	Graeme McCafferty	**Date Reviewed:**	Lent 2023
Date Ratified:	Lent 2023	**Next Review Date:**	Lent 2024
Committee:	Governing Body	**Clerk to the Governors** **Signature:**	Teresa Beard