POLICY TITLE	Data Protection Policy

Policy Area	General
Author	MH
Relevant Statutory Regulations	ISSR Part 3,9; General Data Protection Regulation 2018
Senior Team Lead	
Version	2019.1
Last Updated	May 2019
Review Date	April 2020

Data Protection Policy

1 Aims

1.1 The purpose of this policy is to ensure that the School and all staff, council members and volunteers are aware of their responsibilities under the Data Protection Act 1998.

2 Introduction

2.1 The Privacy Officer is responsible for ensuring information security. This policy applies to all staff, volunteers and governors/trustees.

This policy is for the whole school including the EYFS.

2.2 Initially the School's Application Form and then by signing your Contract of Employment, you have given your consent to the holding, processing and accessing of your personal data for all purposes relating to your employment. These purposes include:

(a) Administering and maintaining personal records.

(b) Providing, administrating and reviewing pay and other benefits (including pension schemes, health insurance and other benefits as may be available from time to time).

(c) Undertaking performance and development reviews.

(d) Maintaining sickness, holiday and other absence records.

(e) Enabling the School to promote and maintain its Equal Opportunities Policy.

(f) Recording CPD and training.

(g) Providing information to Education and governmental bodies, including the Inland Revenue and contributions Agency for social security and other purposes.

(h) Recording the perpetration or alleged perpetration of an offence.

(i) Providing references and information to future employers or external agencies and organisations e.g. mortgage or rental companies.

3 Personal Data

3.1 Personal data covers any information relating to an identified or identifiable natural person including both facts and opinions about an individual. It includes information necessary for employment such as the worker's name and address and details for payment of salary.

Processing of Personal Data

3.2 Unless processing is necessary for the performance of the contract of employment or by law, a worker's consent may be required for the processing of personal data. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the worker. Data may be disclosed to law enforcement (such as the police) and safeguarding agencies (such as the local authority) without consent in certain circumstances such as but not limited to the following examples:

(a) If a parent makes a complaint about a member of staff that the name of the person involved may be passed on to law enforcement and safeguarding agencies.
(b) Information in staff witness statements may be disclosed for purposes of addressing bullying or harassment allegations. Any sensitive personal data asides from names may be redacted.
(c) Where allegations have been made against a member of staff which are reported to staff/social services that the name of the person involved may be passed on to law enforcement and safeguarding agencies.
(d) Where it will ensure the safety of other members of the Roedean community including pupils, staff and members of council, that the name of the person involved may be passed on to law enforcement and safeguarding agencies.
(e) If the School is required to do so by the law. (For safeguarding requirements) Names of relevant persons may be passed on to law enforcement and safeguarding agencies.

3.3 The School may be required by law to submit personal data to HMRC or pension providers.

3.4 Salary data and Bursary/Scholarship information is required by Roedean (Executive Head and DFA) from other schools within the Roedean Group of Schools relating financial reviews and projections.

4 Sensitive Personal Data (Special Category Data)

4.1 The School may, from time to time, be required to process special categories of (sensitive) personal data regarding a worker. Sensitive personal data includes medical information and data relating to gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the worker will generally be required in writing. However, in certain circumstances it may be processed without consent such as where it is required to protect the vital interests of an individual, it is necessary in relation to a legal claim or in some employment contexts.

4.2 Any member of staff collecting or in any way working with personal data must do so in line with the GDPR principles :

(a) Lawfulness, fairness and transparency

(b) Purpose limitation

(c) Data minimisation

(d) Accuracy

(e) Storage limitation

(f) Integrity and confidentiality (security)

(g) Accountability

All Department Heads are required (though the use of the schools established data management framework.) to:

Map all data in use and identify any data processing in use that is likely to result in a high risk to individuals.

Carry out a data protection impact assessment (DPIA) on any data processing in use that is likely to result in a high risk to individuals.

The DPIA process will:

(h) Describe how the information within a data processing operation is collected, stored, used and deleted.
(i) Identify privacy and related risks – catalogue the range of threats, and their related vulnerabilities, to the rights and freedoms of individuals whose data is collected and/or processed.
(j) Identify and evaluate privacy solutions – for each identified risk to the personal data, make a 'risk decision', i.e. whether to accept or reject the risk, whether to transfer it or take steps to reduce the impact or likelihood of the threat successfully exploiting the vulnerability.

The School's Senior Team will be responsible for approving suggested DPIA outcomes and risk management strategies.

5 School Personnel Records

5.1 The following personal data on all employees will be kept:

(a) Name and address, plus contact details of nominated persons to be contacted in the event of an emergency
(b) Bank details, salary history and national insurance number
(c) Details and references relating to previous employment
(d) Sickness, holiday and other absence records
(e) Staff reviews and assessment details, including records of participation in training events
(f) Disciplinary records
(g) Criminal convictions, Disclosure Barring Service Clearance Details
(h) Passport details and identification for DBS applications
(i) Driving Licence, insurance details (for staff using Minibus transport)
(j) Qualification Certificates (copies)

6 Your Rights

6.1 You have the following rights in relation to your personal data:

Subject to a £10 fee, you may make a written request to the Head of School to determine what personal detail is held on you by the School, the purposes for which it is processed and details of those, if any, to whom it has, or may be disclosed. Within 40 days such information shall be supplied in writing except where this would involve a disproportionate effort or both parties agree otherwise.

The School has the right to refuse wholly or in part to comply with the request if:

(a) The release of data would disclose information about another individual
(b) Your request relates to a confidential reference given by the School for, amongst other things, prospective employment.
(c) Your request relates to data processed for the purpose of management forecasting or planning and disclosure would be likely to prejudice the conduct of the School.

6.2 Right to prevent processing which is likely to cause damage or distress

If you believe that the School is processing data in a way which causes, or is likely to cause damage or distress, which is substantial and unwarranted to yourself or another, you have the right to send notice to require that within a reasonable amount of time the processing stops. The School shall reply in writing to confirm that the processing will stop or to state that it believes the processing is justifiable, and the reasons for this assertion. (The damage or distress may be unwarranted if the processing has caused or is likely to cause someone to suffer loss, harm or upset and anguish of a real nature over and above annoyance level without justification).

6.3 Right to prevent processing for the purpose of direct marketing

You are entitled to request that the School ceases or does not commence processing of your personal information for direct marketing.

6.4 Rights in relation to automated decision making

Upon written request, no decision affecting your employment (other than when considering your appointment) shall be based solely on the processing of your data for automatic means. However, if no such notice has been received, but a decision is made in such a way, you will be notified and should make a written request within 21 days if you wish the decision to be reconsidered using different criteria.

7 Your Responsibilities

7.1 You should endeavour to inform the School of any changes to your personal circumstances so your records may be kept up-to-date.

7.2 If you access the personal records of another individual without authority, disciplinary action could be taken against you.

8 Lost Data

8.1 Security breaches must be reported to the Privacy Officer and the IT Manager and dealt with immediately as per the Data Breach Policy.

8.2 Actions that must be carried out include:

(a) Devise a recover and damage limitation plan.

(b) Inform appropriate people and organisations.

(c) Review response and update information security.

9 Data Access Requests

9.1 Please see the Subject Access Request Section with the Privacy Notice for information on how we handle subject access requests.

9.2 Data access requests must be passed to the Privacy Officer immediately on receipt

9.3 Staff should note that ANY comment made in a School email or document can potentially be disclosed. There is NO EXEMPTION for 'embarrassing' comments made about another individual.

10 Personal Data Overseas

10.1 No personal data should be taken overseas (outside of the EU) unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals when processing their personal data.

10.2 Any member of staff who plans to travel to a country outside of the EU with School data must inform the Privacy Officer.

10.3 Any member of staff who intends to transfer school data outside of the EU must inform the Privacy Officer.

10.4 Some of the school's data is stored on servers outside of the EU. In these cases (for example the school's website) arrangements for security and privacy are managed by the IT department and any staff with concerns should notify the Privacy Officer.

11 Roedean Moira House Remote Desktop Service

11.1 Staff wishing to make use of the Remote Desktop service will adhere to these procedures:

(a) You will fill out the online application form available on the staff intranet.

(b) You will be granted access at the discretion of the IT department and only if your answers on the application form meet the required criteria.

(c) You agree to abide by the usage terms in the application form at all times (you may also be asked to agree to an updated set of usage terms at a later date).

12 Breach of Policy

12.1 Any breaches of this policy may result in disciplinary action, and for more serious breaches dismissal.

13 Central Data Retention Periods

13.1 Bursary

(a) Correspondence to be destroyed after 10 years.

(b) Digital financial records to be destroyed after 10 years.

(c) Invoices and petty cash slips to be destroyed after 6 years.

13.2 SCHOOL OFFICE

(a) Pupil paper files to be destroyed after 7 years.

(b) Correspondence and digital files to be destroyed after 10 years.

13.3 GENERAL – ALL OTHER DEPARTMENTS OR DATA TYPES

(a) Paper and digital files containing personal data to be destroyed after 10 years.