KINGS MONKTON SCHOOL

Kings Monkton School

Data Protection Policy

September 2019

Introduction

This Policy sets out the obligations of Kings Monkton School Limited ("the Company") regarding data protection and the rights of pupils, parents, staff and visitors ("data subjects") in respect of their personal data under the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27th April 2016, application date 25th May 2018 ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a 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.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by Kings Monkton School, its employees, agents, contractors, or other parties working on behalf of the Company.

Kings Monkton school is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Data Protection Principles

1. This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a. processed lawfully, fairly, and in a transparent manner in relation to the data subject;

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 it is processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is 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 is 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 Regulation in order to safeguard the rights and freedoms of the data subject;

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.

Lawful, Fair, and Transparent Data Processing

2. The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more

specific purposes;

b. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c. processing is necessary for compliance with a legal obligation to which the controller is subject;

d. processing is necessary to protect the vital interests of the data subject or of another natural person;

e. 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 controller;

f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Processed for Specified, Explicit and Legitimate Purposes

3. Kings Monkton School collects and processes the personal data set out in Part 22 of this Policy. This may include personal data received directly from data subjects (for example, pupil and family contact details) and data received from third parties (for example, pupil files from previous schools including Common Transfer Files (CTF)).

4. The School only processes personal data for the specific purposes set out in Part 22 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

Adequate, Relevant and Limited Data Processing

5. Kings Monkton School shall only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4 above.

Accuracy of Data and Keeping Data Up to Date

6. Kings Monkton School shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular, or at least six monthly intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Timely Processing

7. Kings Monkton School shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

Secure Processing

8. Kings Monkton School shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 23 and 24 of this Policy.

Accountability

9. Kings Monkton School's data protection officer (DPO) is Mrs Nicola Parry-Belcher, Business Manager (e-mail: nicolaparrybelcher@kingsmonkton.org.uk).

10. Kings Monkton School shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a. The name and details of the Company, its DPO, and any applicable third party data controllers;

b. The purposes for which Kings Monkton school processes personal data;

c. Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;

d. Details (and categories) of any third parties that will receive personal data from the Company;

e. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

f. Details of how long personal data will be retained by the Company; and

g. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Privacy Impact Assessments

11. The Company shall carry out Privacy Impact Assessments when and as required under the Regulation; template is at Annex A. Privacy Impact Assessments shall be overseen by the Company's DPO and shall address the following areas of importance.

a. The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

b. Details of the legitimate interests being pursued by the Company;

c. An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

d. An assessment of the risks posed to individual data subjects; and

e. Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

The Rights of Data Subjects

12. The Regulation sets out the following rights applicable to data subjects:

a. The right to be informed;

b. The right of access;

c. The right to rectification;

d. The right to erasure (also known as the 'right to be forgotten');

e. The right to restrict processing;

f. The right to data portability;

g. The right to object;

h. Rights with respect to profiling and means-testing.

Keeping Data Subjects Informed

13. Kings Monkton School will ensure that the following information is provided to every data subject when personal data is collected:

a. Details of the Company including, but not limited to, the identity of Mrs Nicola Parry-Belcher, Business Manager, its DPO;

b. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 22 of this Policy) and the legal basis justifying that collection and processing;

c. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e. Where the personal data is to be transferred to one or more third parties, details of those parties;

f. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);

g. Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

h. Details of the data subject's rights under the Regulation;

i. Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j. Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

k. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

l. Details of any decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

m. The information set out above in Part 13 shall be provided to the data subject at the following applicable time:

1) Where the personal data is obtained from the data subject directly, at the time of collection (such as upon Registration);

2) Where the personal data is not obtained from the data subject directly (i.e. from another party):

3) If the personal data is used to communicate with the data subject, at the time of the first communication; or

4) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

5) In any event, not more than one month after the time at which the Company obtains the personal data.

Data Subject Access

14. A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. Kings Monkton School will normally respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension). All subject access requests received must be forwarded to Mrs Nicola Parry-Belcher the Company's data protection officer. (E-mail: nicolaparrybelcher@kingsmonkton.org.uk).

15. Kings Monkton school does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

16. The Education (Independent School Standards) Regulations 2014 set out certain minimum standards that all independent schools must meet. The standards on information provision require that an annual written report of each registered pupil's progress and attainment in the main subject areas taught is provided to the parents of that registered child. Kings Monkton School give access to parents and pupils their full and interim reports, however do not give access to the pupil's educational record.

Rectification of Personal Data

17. If a data subject informs Kings Monkton School that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension). In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

Erasure of Personal Data

18. Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

1) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;

2) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

3) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);

4) The personal data has been processed unlawfully;

5) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

19. Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall

be informed of the need for the extension). In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

20. Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Objections to Personal Data Processing

21. Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes. Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith. Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Means Testing

22. Where Kings Monkton School uses personal data for Means-Testing, with regard to Bursary awards, hardship applications and general reduction in fees, the following shall apply:

a. Clear information explaining the means-testing will be provided, including its significance and the likely consequences (detailed in application packs);

b. Appropriate mathematical or statistical procedures will be used;

c. Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d. All personal data processed for means-testing purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 23 and 24 of this Policy for more details on data security).

Personal Data

23. The following personal data may be collected, held, and processed by the Company:

a. General information on prospective and current pupils and their families, including personal information, identification and medical details, in order to process application, manage attendance and provide appropriate care and support;

b. Performance data (including grades achieved, target grades, aspirational grades and any academic concerns) on pupils in order to provide the best educational experience possible;

c. SEN data including Local Authority funding agreements, Personal Support Plans, medical and

psychological reports, Additional Needs Statements and interventions information.

d. Information on staff (general personal information, medical questionnaires, emergency contact details, bank details, copies of awarded certificates/qualifications, references, evidence supplied for a DBS application), in order to comply with HR regulations, gather information for payroll and ensure suitability for the position applied for.

e. CCTV images will be collected externally for security reasons and internally for health & safety.

Data Protection Measures

24. Kings Monkton School shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a. All emails containing personal data must be encrypted. Subjects must be referred to by initials only, or coded references (as supplied by the School's Administrative Office).

b. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using AVG SHRED. Shredders are available in the Administrative office, Business Management office, Principal's office, Vice-Principal's office and SENCo office.

c. Personal data may be transmitted over secure/monitored networks only (Kings Monkton Microsoft Outlook accounts); transmission over unsecured networks is not permitted in any circumstances (including via personal emails);

d. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

e. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. All temporary files associated therewith should also be deleted;

f. Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

g. Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Special Delivery Guaranteed.

h. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the DPO or Miss Rachael Newby, Office Manager.

i. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar. Archived data will be similarly secured either on-site or appropriately outsourced;

j. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the DPO. All reference requests are to be dealt with centrally through the Administrative office;

k. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time. Desks in public areas or those with open access should be kept clear of any personal data. Private offices must be secured at all times;

l. If personal data is being viewed on a computer screen and the computer in question is to be left

unattended for any period of time, the user must lock the computer and screen before leaving it. All Kings Monkton School computers are to be set to hibernate mode after no longer than five minutes, networked printers are to be locked immediately after use;

m. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Kings Monkton School or otherwise without the formal written approval of the data protection officer, Mrs Nicola Parry-Belcher, and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary**.**

n. If memory sticks, or other digital data storage devices, are used they must be encrypted. Encrypted devices can be requested from the DPO.

n. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

o. All personal data stored electronically should be backed up via Shadow Copy three times a day and external back-up once a night with back-ups stored offsite. All backups will be encrypted: authentication for onsite back-up and encrypted bitlocker key for offsite.

p. All electronic copies of personal data should be stored securely using passwords;

q. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols**;**

r. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

s. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Ms Rachael Newby, Office Manager, to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least every 6-months.

Organisational Measures

25. Kings Monkton School will ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a. All employees, agents, contractors, or other parties working on behalf of the Company are to read and acknowledge the School's visitors information booklet. In doing so they will be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy. They will be offered a copy of this policy;

b. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

c. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will undertake GDPR continuous professional development annually;

d. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

e. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed. Formal reviews of all organisational processes will be undertaken on a 6-monthly basis by the DPO;

f. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

e. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract.

f. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be required to confirm understanding of this policy on an annual basis. Certificate at Annex B;

f. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;

g. Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

h. Kings Monkton School will undertake a formal Data Protection Audit as required, at least on an annual basis, in order to ensure adherence to this policy;

Transferring Personal Data to a Country Outside the EEA

26. Kings Monkton School may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c. The transfer is made with the informed consent of the relevant data subject(s);

d. The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

e. The transfer is necessary for important public interest reasons;

f. The transfer is necessary for the conduct of legal claims;

g. The transfer is necessary to protect the vital interests of the data subject or other individuals where

the data subject is physically or legally unable to give their consent; or

h. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

27. All personal data breaches must be reported immediately to the Company's DPO. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

28. Data breach notifications shall include the following information:

a. The categories and approximate number of data subjects concerned;

b. The categories and approximate number of personal data records concerned;

c. The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d. The likely consequences of the breach;

e. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy

29. This Policy shall be deemed effective as of 2nd September 2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Mr Paul Norton
Position:	Director and Principal, Kings Monkton School
Date:	2nd September 2019
Due for Review by:	31st August 2020
Signature:	

Annexes:

A. Privacy Impact Assessment Template.
B. Data Protection Statement.

Privacy Impact Assessment (PIA)

In accordance with Conducting Privacy Impact Assessments Code of Practice, ICO. 20140225, Version 1.0.

Step One: Identify the need for an PIA

Explain what Kings Monkton School aims to achieve, what the benefits will be to the organisation, to individuals and other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal.
Summarise why the need for a PIA was identified (screening questions).

Step Two: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also identify how many individuals may be affected by the project.

Step Three: Consultation Requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to relevant stages of your project management process.

Consultation can be used at any stage of the PIA process.

Step Four: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance corporate risks. Larger-scale PIAs might record this information on a formal risk register.

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Organisation/Corporate Risk

Step Five: Sign off and record the PIA outcomes

Who has approved the privacy risks to the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By

Step Six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that may have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for actions

Point of contact for future privacy concerns

Data Protection Statement

Policy Receipt Acknowledgement for the Kings Monkton Data Protection Policy

In effect: September 2019 until further notice

I have read and been informed about the content, requirements, and expectations of the Kings Monkton Independent School Data Protection policy. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my employment and my continuing employment with Kings Monkton School.

I understand that if I have questions, at any time, regarding the dress code policy, I will consult with my immediate line manager or the Data Protection Officer.

Please read the Data Protection policy carefully to ensure that you understand the policy before signing this document.

Employee Signature: _____

Employee Printed Name: _____

Date: _____