Marylebone Boys' School

STUDIO ET INDUSTRIA

Data Protection Policy

Policy Name	Data Protection Policy
Author	Paul Green
Last reviewed	January 2024
Next review date	January 2027
Required to publish on school website	Yes
Statutory	Yes
Data Protection Officer (DPO)	John Pearson-Hicks (Grow Education Partners Ltd)

Contents:

Statement of intent

Marylebone Boys' School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018)
The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.
This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.
Organisational methods for keeping data secure are imperative, and Marylebone Boys' School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy meets the current requirements of UK Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR, GDPR (UK) and DPA 2018. It is also based on the information provided by the Article 29 Working Party.

Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information. This policy complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Legal framework

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

- The UK General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005
- 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 Guide to Data Protection
- This policy will be implemented in conjunction with the following other school policies:
    - **Photography and Videos at School Policy**
    - **E-security Policy**
    - **Freedom of Information Policy**
    - **CCTV Policy**

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.

There are additional conditions for processing certain sensitive data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person and data concerning health or a natural person's sex life or sexual orientation; the Data Protection refers to these as special categories data.

Principles

In accordance with the requirements outlined in the Data Protection, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- 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.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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 the data subject.
- 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.

The Data Protection also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles". Where a request is received the school will cooperate with the Information Commissioner's Office (ICO).

Third Party Processors

Where processing is to be carried out on behalf of the school, the school shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

Accountability

The school will implement appropriate technical and organisational measures to ensure and be able to demonstrate that data is processed in line with the principles set out in the GDPR.

1.1. The school will 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 or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation, and the Data Protection Officer (DPO)
- Purpose(s) of the processing

- Description of the categories of data subjects and personal data
- Retention schedules where possible
- 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 will implement 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.
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

Data protection officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with Data Protection.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members. An existing employee may be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
- Act as the contact point for the ICO on issues relating to processing
- Ensure that MBS is correctly registered with the ICO and act as the contact point for the ICO on issues relating to processing.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the headteacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

The school will act as a data processor; however, this role may also be undertaken by other third parties.

In accordance with the GDPR, the school will only process data lawfully, that is if and to the extent that at least one of the following applies:

- 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 natural person.

Special categories data will only be processed under the following conditions, and within the parameters set out in Article 9 of the GDPR:

- Explicit consent of the data subject, unless reliance on consent is prohibited domestic law.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations and exercising specific rights of the school or the data subject under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another natural person 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 domestic 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 domestic 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) (as supplemented by section 19 of the 2018 Act) and subject as provided in Article 9.3.

Consent

Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

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 data subject at any time.

Where a child is under the age of 16 the consent of holder of parental responsibility will be sought prior to the processing of the child's data, except where the processing is related to preventative or counselling services offered directly to a child.

When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be gained from pupils where it is deemed that the pupil has a sound understanding of what they are consenting to.

The right to be informed

Information 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 information is written in a clear, plain manner that the child will understand.

In relation to personal 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 contact details of the controller (the school), and where applicable, the controller's representative, as well as the DPO.
- The purpose of, and the legal basis for, processing the data.
- Any recipient or categories of recipients of the personal data.
- If applicable 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:
  - Withdraw consent at any time.
  - Request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.
  - 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.
- Information on any further processing of the data for a purpose other than that for which it was collected.

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, 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 categories of personal data that the school holds, the source that 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 data subject, at the latest, when the first communication takes place.

Provided that such information need not be supplied where the data subject already has it or its provision would involve a disproportionate effort or it is required to be kept confidential, as more particularly described in Article 14.5.

The right of access

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

Data subjects 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 data subject 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 data subject 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 data subject 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 a data subject, the school will ask the data subject to specify the information the request is in relation to.

The right to rectification

Data subjects 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 data subject 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 data subject, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

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

Data subjects 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 data subject withdraws their consent and there is no other legal grounds for the processing
- When the data subject objects to the processing pursuant to Article 21(1) 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 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
- To comply with a legal obligation or 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.

The right to restrict processing

Data subjects 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, without the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest, guaranteeing that just enough information about the data subject 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 a data subject contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where a data subject 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 data subject opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the data subject 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 data subjects when a restriction on processing has been lifted.

The right to data portability

Data subjects 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 a data subject has provided to a controller
- Where the processing is based on the data subject'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 data subject.

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 data subject, the school will consider whether providing the information would prejudice the rights of any other data subject.

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 timeframe can be extended by two months, ensuring that the data subject 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 data subject the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The school will inform data subjects 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.

Data subjects 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:

- A data subject's grounds for objecting must relate to his or her particular situation.

- The school will stop processing the data subject'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 a data subject's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The data subject 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 data subjects to object online.

Automated decision making and profiling

Subject to Article 22(2), data subjects have the right not to be subject to a decision when:

- It is based solely on automated processing, e.g. profiling, and
- It produces a legal effect or a similarly significant effect on the data subject.

The school will take steps to ensure that data subjects are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the data subject and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of special categories data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of domestic law.

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 carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. When carrying out a DPIA the school will seek the advice of the DPO.

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 the school's reputation which might otherwise occur.

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 data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

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 data subjects
- 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.

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.

Where a breach is believed to have occurred the DPO will carry out a Data Breach Impact Assessment which will establish what has happened, evaluate the severity of the impact and decide what action needs to be taken and whether the breach is notifiable.

All potential breaches will be recorded in the Data Protection Log. It will be assigned an internal reference number and all associated document will be stored with it.

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

Where a breach is likely to result in a risk to the rights and freedoms of data subjects, the ICO will be informed.

All notifiable breaches will be reported to the ICO within 72 hours of the school becoming aware of them.

The risk of the breach having a detrimental effect on the data subject, and the need to notify the ICO, 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 the data subject without undue delay, subject only to Article 34.3.

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 ICO 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 data subjects 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 to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

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, mobile devices 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.

Where visitors are present at formal meetings, where confidential and/or personal information, is being discussed, the chair of the meeting will take responsibility for ensuring that all present are reminded of their responsibility to protect the data and will be responsible for collecting and destroying any papers that contain confidential or personal information.

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 Data Protection seriously and any unauthorised disclosure may result in disciplinary action.

The school business manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

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
- Minutes of meetings
- 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.

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 DPO is responsible for keeping the records secure and allowing access.

The school will always indicate its intentions for taking photographs of pupils and will receive 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.

Precautions, as outlined in the Photography and Videos at School Policy, are taken when publishing photographs of pupils, in print, video or on the school website.

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

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.

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.

Policy review

The DPO is responsible for monitoring and reviewing this policy as part of the general auditing and compliance work, they carry out. They will work with the School Data Protection Lead and the Governing Board to ensure that this policy remains contemporaneous and appropriate. This policy will be reviewed yearly, and changes recommended when

appropriate. The Governing Board will be asked to sign off the policy review and any necessary changes.

The next scheduled review date for this policy is June 2022.

Appendix 1

GDPR privacy notice for pupils and parents

Marylebone Boys' School
STUDIO ET INDUSTRIA

Privacy notice for students and parents

This privacy notice is written for both students and their parents/carers at Marylebone Boys' School and explains how we collect, store and use personal data about our students.

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

We, Marylebone Boys' School, are the 'data controller' for the purposes of data protection law.

The Data Protection Officer (DPO) is John Pearson-Hicks. (john.pearson-hicks@london.anglican.org)

The school data protection lead is Paul Green (dpo@maryleboneschool.org)

The personal data we hold

Personal data that we may collect, use store and share (when appropriate) about students includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Student and curricular records
- Characteristics, such as ethnicity, language, nationality, country of birth, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information (Such as sessions attended, number of absences and absence reasons)
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in the school.
- Catering information such as food/drinks purchased
- Biometric Data (fingerprint recognition system)

We may also hold data about students that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support student learning
- Monitor and report on student progress
- Provide appropriate pastoral care
- Assess how well our school is doing

- Protect student welfare and ensure the safety of the school site
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data
We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use personal information where:
Students or parents/carers have given us permission to use it in a certain way:

- We need to protect your interests (or someone else's interest)
- Where we have got permission to use your data, you or your parents/carers may withdraw this at any time.

We will make this clear when we ask for permission, and explain how to go about withdrawing consent.
Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information
Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis.
In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data
We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.
We have a record retention schedule/records management policy which sets out how long we must keep information about student.

Data sharing
We do not share personal information about you with anyone outside the school without permission from student or parents/carers, unless the law and our policies allow us to do so.
Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about student' safety and exclusions
- The Department for Education (a government department)
- Your family and representatives
- Schools, colleges, examining bodies and other places of education

- Our regulator (the organisation or "watchdog" that supervises us), e.g. Ofsted, Independent Schools Inspectorate
- Suppliers and service providers – so that they can provide the services we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Student Database

We are required to provide information about students to the Department for Education as part of statutory data collections such as the school census For further information please see:
https://www.gov.uk/education/data-collection-and-censuses-for-schools
Some of this information is then stored in the National Student Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.
The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.
You can also contact the Department for Education with any further questions about the NPD
https://www.gov.uk/contact-dfe

Youth support services

Once our pupils reach the age of 13, we also pass pupil information to our local authority (LA) and/or provider of youth support services because they have responsibilities in relation to the education or training of 13 to 19-year-olds under section 507B of the Education Act 1996.
Sharing this information allows them to provide the following services:

- Youth support services
- Careers advisers
- Post-16 education and training providers

The information we share is limited to the pupil's name, address and date of birth; however, where a parent has provided their consent, other relevant information will be shared – this right to consent is transferred to pupils once they reach 16-years-old.

Sharing by the DfE

The DfE is legally allowed to share pupils' personal information with certain third parties, including the following:

- Schools
- LAs
- Researchers
- Organisations connected with promoting the education or wellbeing of pupils
- Other government departments and agencies
- Organisations fighting or identifying crime

Organisations fighting or identifying crime, such as the Home Office and the police, may use their legal powers to contact the DfE to request access to individual level information relating to detecting a crime. The DfE typically supplies information on

around 600 pupils per year to the Home Office and approximately one per year to the police.
For more information about how the DfE collects and shares pupil information, you can look at the information in the following two links:

- https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

- https://www.gov.uk/government/publications/dfe-external-data-shares

What are your rights?

You have specific rights to the processing of your data, these are the right to:

- Request access to the information the school holds about you.
- Object to the processing of your information that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.
- Lodge a complaint with the ICO.

If you want to request access to the personal information that we have about you, please contact the DPO at the following address dpo@maryleboneschool.org
If you are concerned about the way we are collecting or using your information, please raise your concern with the school's DPO in the first instance. You can also contact the ICO at:
https://ico.org.uk/concerns/

Appendix 2

GDPR privacy notice for the school workforce

Marylebone Boys' School
STUDIO ET INDUSTRIA

Who processes your information?

The school is the data controller of the personal information you provide to us. This means it determines the purposes for which, and the manner in which, any personal data relating to staff is to be processed.

Where necessary, third parties may be responsible for processing staff members' personal information. Where this is required, the school places data protection requirements on third party processors to ensure data is processed in line with staff members' privacy rights.

Why do we need your information?

Marylebone Boys' School has the legal right and a legitimate interest to collect and process personal data relating to those we employ to work at the school, or those otherwise contracted to work at the school. We process personal data in order to meet the safeguarding requirements set out in UK employment and childcare law, including those in relation to the following:

- Academy Funding Agreement
- Academy's legal framework
- Safeguarding Vulnerable Groups Act 2006
- The Childcare (Disqualification) Regulations 2009

Staff members' personal data is also processed to assist in the running of the school, and to enable individuals to be paid.

If staff members fail to provide their personal data, there may be significant consequences. This includes the following:

Employment checks:

Failure to provide the school with ample proof of a right to work in the UK will prevent employment at Marylebone Boys' School.

Employees found to be working illegally could face prosecution by law enforcement officers.

Salary requirements:

Failure to provide accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or an employee paying too much tax.

For which purposes are your personal data processed?

In accordance with the above, staff members' personal data is used for the following reasons:

- Contractual requirements
- Employment checks
- Salary requirements

Which data is collected?

The personal data the school will collect from the school workforce includes the following:

- Names
- National insurance numbers
- Special characteristics such as gender, age, ethnic group
- Employment contract information
- Remuneration details
- Qualifications
- Absence information (number of absences and reason)

We routinely share this information with the Department for Education (DfE) and our local authority (LA). The collection of personal information will benefit both the DfE and LA by:

- Improving the management of workforce data across the education sector.
- Enabling the development of a comprehensive picture of the workforce and how it is deployed.
- Informing the development of recruitment and retention policies.
- Allowing better financial modelling and planning.
- Enabling ethnicity and disability monitoring.
- Supporting the work of the school teachers' review body.

Will your personal data be sought from third parties?

Staff members' personal data is only sought from the data subject. No third parties will be contacted to obtain staff members' personal data without the data subject's consent.

How is your information shared?

Marylebone Boys' School will not share your personal information with any third parties without your consent, unless the law allows us to do so. We are required, by law, to pass on some personal information to our local authority and the Department for Education.

How long is your data retained for?

Staff members' personal data is retained in line with the schools' Records Management Policy. Data will only be retained for as long as is necessary to fulfil the purposes for which it was processed, and will not be retained indefinitely.

If you require further information regarding retention of data, and the periods for which your personal data is held, please refer to the school's Records Management Policy.

What are your rights?

As the data subject, you have specific rights to the processing of your data.

You have a legal right to:

- Request access to the personal data that Marylebone Boys' School holds.
- Request that your personal data is amended.
- Request that your personal data is erased.
- Request that the processing of your data is restricted.

Where the processing of your data is based on your explicit consent, you have the right to withdraw this consent at any time. This will not affect any personal data that has been processed prior to withdrawing consent.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Staff members also have the right to lodge a complaint with the Information Commissioner's Office (ICO) in relation to how Marylebone Boys' School processes their personal data.

How can you find out more information?

If you require further information about how we and the Department for Education store and use your personal data, please visit the Gov.UK website, or refer to the school's GDPR Data Protection Policy and Records Management Policy.

Declaration

I, _____, declare that I understand:

- Marylebone Boys' School has a legal and legitimate interest to collect and process my personal data in order to meet statutory and contractual requirements.

- There may be significant consequences if I fail to provide the personal data Marylebone Boys' School requires.
- Marylebone Boys' School may share my data with the Department for Education, and subsequently the local authority.
- Marylebone Boys' School will not share my data to any other third parties without my consent, unless the law requires the school to do so.
- The nature and personal categories of this data, and where the personal data originates from, where my data is obtained from third parties.
- My data is retained in line with Marylebone Boys' School's Records Management Policy.
- My rights to the processing of my personal data.

Name of staff member: _____

Signature of staff member: _____

Date: _____