DATA PROTECTION POLICY

HARROW SCHOOL

1. INTRODUCTION

The School means Harrow School as now or in the future constituted. The School is constituted as a Royal Charter Corporation known as The Keepers and Governors of the Possessions Revenues and Goods of the Free Grammar School of John Lyon ("We"). We are a charity registered in England and Wales with registration number 310033. We have our office at Harrow School, 5 High Street, Harrow on the Hill, Middlesex HA1 3HP. For the purposes of the (2018) Act, the School is the "data controller" of personal data.

This Data Protection Policy defines how the School will meet its obligations with regards to personal data, as required by the Data Protection Act 2018 (the 'Act') and the EU General Data Protection Regulations (the 'GDPR').

If you are unsure about any aspect of this Policy or your responsibilities, please contact your line manager and/or the Privacy Officer at privacyofficer@harrowschool.org.uk.

2. SCOPE

All employees, contractors, agents, consultants, partners or other members of the School who have access to any personal data held by or on behalf of the School, must comply with this Policy and any supporting policies, procedures and guidance in order to meet duties and responsibilities.

This policy should be read alongside any contract of employment (or contract for services) and any other notice we issue from time-to-time in relation to your data. This policy forms part of the terms and conditions of all employees' contracts of employment. A breach of the policy may be regarded as misconduct, leading to disciplinary action up to and including summary dismissal. See Appendix A for a list of supporting policies, procedures and guidance and Appendix B for a list of key definitions.

Policy also covers staff and workers engaged by:

- Harrow School Enterprises Limited (HSEL)
- The Harrow Association (HA)
- The Harrow Development Trust (HDT)

In order to operate safely and efficiently, the School has to collect and use personal data about people with whom it works ("data subjects") for the purposes set forth under this Policy and any supporting policies and procedures.

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

The School may need to process special category personal data (concerning health, ethnicity, religious or philosophical beliefs, genetic or biometric data, sexual orientation) or criminal records information such as criminal convictions and offences in accordance with the rights and duties imposed on it by law, or from time to time by explicit consent where required or subject to the legal exemptions.

The School regards the lawful and fair treatment of personal data as very important to its successful operations and to maintaining confidence between the School, its staff and those with whom it carries out business. To this end the School fully endorses and adheres to the Principles of Data Protection as set out in the Act and GDPR.

Lawful bases for the School to process personal data based on the Act and the GDPR.

The School processes personal data:

- Where the data subject has given consent to the processing of his or her personal data for one or more specific purposes,
- Where processing is necessary for the performance of a contract (entering into employments contract, third party contracts etc.),
- Where processing is necessary for compliance with a legal obligation to which the School is subject (employment law requirements, assisting criminal investigations etc.),
- Where processing is necessary in order to protect the vital interests of the data subject or of another natural person (in situations where a data subject has a severe accident or illness at the School premises and needs immediate medical support),
- Where 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 School,
- Where processing is necessary for the purposes of the legitimate interests the School (including but not restricted to: administering the School to the highest standards, providing the best education possible, increasing communications between the School, alumni and parents for fundraising purposes, and evaluation of employees' performances).

3. POLICY COMMITMENTS FOR PROCESSING PERSONAL DATA

The School has made the following policy commitments for processing personal data:

- There is someone with specific responsibility for data protection in the School;
- Everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice in accordance with the rules and requirements of the Act and the GDPR and the rules set forth under this Policy and any supporting policies;
- We seek to train appropriately and to supervise all those who manage and handle personal data;
- Everyone managing and handling personal data is appropriately supervised;
- Anyone making enquiries about either their own personal data or the handling of it, whether a member of staff or a member of the public, will have their enquiry handled in accordance with the School's Subject Access Request procedures;
- Queries about handling personal data are promptly and courteously dealt with;
- Methods of handling personal data are regularly assessed and evaluated;
- Data sharing with third parties is carried out under a written agreement, setting out the scope and limits of the sharing in accordance with the principles of the Act and the GDPR. Any disclosure of personal data will be in compliance with approved procedures;
- Where the School transfers personal data outside of the EEA, it will do so using the appropriate transfer mechanisms and will ensure that the necessary protections are in place for the the security of personal data;
- Observe in full conditions regarding the fair collection and use of personal data;
- Meet its legal obligations to specify the purpose for which personal data is used;
- Collect and process appropriate personal data and only based on the legal grounds set forth under this Policy and any supporting policies to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of personal data used;
- Apply retention procedures to determine the length of time personal data is held;
- Take appropriate technical and organisational security measures to safeguard personal data as outlined in the School's ICT policies;
- Ensure that the rights of people about whom the personal data is held can be fully exercised under the Act and the GDPR;
- Implement Data Protection Impact Assessments (DPIAs) in high-risk situations (where we process large amounts of personal or sensitive data e.g. health, religion,ethnicity etc.) or any other major project which requires the processing of personal data, and meet its Data Protection by Design and Default obligations;
- Personal data must be processed in line with data subjects' rights; and

- The School ensures that all personal data is as up-to-date and accurate as possible and that data subjects or parents/guardians know to inform the School of any significant changes to important information such as contact details and bank details held about them.

4. ROLES AND RESPONSIBILITIES

The following roles and responsibilities apply:

Corporation IT Committee

The Corporation IT Committee is the successor to the Foundation IT Committee (FIC), focussing solely on Corporation IT matters, with the objective of comparing and promoting best practice across the Corporation.

IT and Data Steering Committee

The Committee will have oversight of the Data Management Committee (DMC), the IT Operations Committee (Academic & Pastoral) (IT Ops) and the Support IT Operations Committee (SITOps). The Committee will be the approving authority for all IT budget bids from the DMC, IT Ops and SITOps and will approve data privacy policies. It will seek to share best practice with the John Lyon School.

Data Management Committee

The DMC ensure departmental compliance with data privacy legislation and promote good practice across the School and related entities, encourage cultural change to embed good data privacy practice in the staff and identify related training needs.

Support IT Operations Committee

The purpose is to coordinate the use of IT in Support departments, look at significant new projects and liaise with the IT and Data Steering Committee (IT&DSC) and Data Management Committee (DMC), to approve support budget requests to the IT&DSC and to ensure legislation, guidance, recommendations and best-practice are taken into account in all decision-making.

IT Operations Committee

This committee comprises the Deputy Head Master, The Director of Studies, the Director of Pastoral Care and the Director of IT. The committee meets every two weeks to review the more day-to-day operational issues that impact boys' learning and wellbeing.

Privacy Officer

The School has engaged Privacy Culture to take on the role of Privacy Officer. They will endeavour to ensure that personal data is processed in compliance with the Policy and the principles of the Data Protection Act and GDPR. The Privacy Officer will be supported in their role by the Committees outlined above.

All staff must comply with this Policy and any related policies, procedures and guidance in the conduct of their duties and responsibilities.

5. PRIVACY INFORMATION AND FAIR PROCESSING

'Processing' involves collection, recording, organising, structuring or storage; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; alignment or combination; and restriction, destruction or erasure. This includes processing personal data which forms part of a filing system and any automated processing.

The School will ensure that all points at which personal data is collected will have a Privacy Notice; these will contain sufficient privacy information to inform the data subject about the collection and use of their personal data. The Privacy Officer will maintain the list of Privacy Notices.

The key Privacy Notices will be:

- Staff Privacy Notice
- (Parent and Pupil) Privacy Notice (as referred to in the Standard Terms and Conditions)

Any member of staff wishing to collect personal data should consult their Departmental representative and/or the Privacy Officer to check whether an existing Privacy Notice already provides sufficient privacy information.

The School will maintain a Photography Policy for Pupils and Staff, outlining the cases where it will rely on legitimate interests or consent to process photographs.

5. TRAINING

The Privacy Officer will arrange appropriate training for members of the School's staff and enforce the monitoring and review of this policy. Training records will be maintained to evidence compliance.

6. WORKING WITH SUPPLIERS, CONSULTANTS AND PARTNERS

In order to ensure the School meets its obligations to manage and protect personal data:

- due diligence must be undertaken on all suppliers, consultants and partners who will handle (process) personal data on behalf of the School, and
- any contract, processing or data sharing agreements signed between the School and a supplier, consultant and/or partner must contain the appropriate clauses.

No contract or data sharing agreement should therefore be entered into without sufficient due diligence and the appropriate clauses in place.

Staff must consult their Departmental representative and/or the Privacy Officer before any contract or data sharing agreement is signed.

7. HANDLING SUBJECT ACCESS REQUESTS (SARS) AND OTHER RIGHTS REQUESTS

Data subjects have a number of rights. The full list can be found in Appendix C; the main rights are to

- Request access to data about them held by the School;
- Prevent processing in certain circumstances such as for direct marketing purposes or where the processing relies on legitimate interests;
- Have inaccurate data about them amended;
- Request deletion of the data held by the School; and
- Object to data processing activities of the School that have disproportionate impact on their rights.

On receipt of a formal request, it should be immediately passed to the departmental representative and/or the Privacy Officer. This will ensure that:

- the request can be processed in accordance with the appropriate procedure;
- the required checks and searches can be undertaken;
- if required, exemptions applied, and
- a compliant response can be provided.

Routine disclosures of personal data should be undertaken in accordance with agreed departmental procedures; see Section 8 below.

More detailed information can be found in the School's Subject Access Request Procedure.

8. ROUTINE DISCLOSURES AND USES OF PERSONAL DATA

School Departments may need to share and access personal data to provide services or deliver their functions. Also, the School may receive requests from third parties to disclose personal data it holds about data subjects.

- The routine collection, use, disclosure and storage of personal data must be for legitimate purposes as defined in the Records of Processing Activity (ROPA) and Record Retention Schedule.

Staff will not disclose personal data unless the individual has given their consent; there is a legitimate and established need, or one of the specific exemptions under the Act applies.

For example, disclosures can occur in connection with:

- Safeguarding;
- The prevention or detection of crime;
- assessment or collection of any tax or duty;
- Where necessary to exercise a right or obligation conferred or imposed by law upon the School and
- References given by the School.

For example, personal data may be withheld if:

- It would cause serious harm to the physical or mental health of the employee or another individual, or
- given to a court in proceedings in Magistrates' Courts.

Staff must seek advice and guidance from their departmental representative and/or the Privacy Officer if they have any doubt about whether the collection, use, disclosure and/or storage of personal data is for a legitimate purpose.

9. SECURITY OF PERSONAL DATA

All staff must adhere to the following School Policies:

- Staff ICT Acceptable Use Policy
- Information Security Policy
- Archive Policy

10. RECORDS RETENTION, DISPOSAL AND DATA ACCURACY

The School will endeavour to ensure that all personal data held in relation to data subjects is accurate. This applies to the data held for boys and staff. The School makes clear that the burden of responsibility for accuracy of information held lies with the data subject e.g. it makes clear to parents that they must update the School about any changes to their son's personal data and asks the same of staff.

- Staff must notify the HR Department of any changes to personal data held about them.
- Staff must update personal data when they become aware it has become inaccurate.
- Parents & Pupils must notify the School of any changes to personal data by notifying the House Master, the Data Manager or the Medical Centre, as appropriate.

The School will maintain a Records Management Policy and Data Retention Schedule to meet the School's obligation to not retain personal data for longer than is necessary for the purposes for which it was collected. When requested, staff should work with the Records Manager & Archivist to ensure adherence to the Records Management Policy and Data Retention Schedule.

11. DATA BREACH MANAGEMENT

The Privacy Officer will assist the School in assessing any and all breaches and decide whether it needs to report them to the Information Commissioner's Office (ICO) within 72 hours in accordance with the School's Data Breach Management Procedure. The School will follow the advice provided by the Information Commissioner's Office on how to manage data breaches and when to notify.

All members of staff must immediately (as soon as they are aware) report any and all suspected or actual breaches to the Privacy Officer, retaining any evidence in relation to the breach and sharing this forward as required.

Breaches should be reported as follows:

- IT-related – inform the IT service desk (who will then report it to the Privacy Officer)

- Non-IT related – inform your line manager (who will then report to the Privacy Officer)

The Privacy Officer will then liaise with the Department Representative to manage the breach in accordance with the School's Data Breach Procedure.

Examples of breaches can be found in Appendix D.

12. NOTIFICATION TO THE INFORMATION COMMISSIONER

The Data Protection Act 2018 and the GDPR requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Privacy Officer will be responsible for this task. To this end Departments will be responsible for notifying and updating the Privacy Officer of the processing of personal data, within their area.

The School's Privacy Officer will review the Data Protection Register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes made between reviews will be brought to the attention of the School's Privacy Officer immediately.

13. ENFORCEMENT

If an individual believes that the School has not complied with this Policy or acted in accordance with the Data Protection Act or GDPR, he or she should notify the School's Privacy Officer. If an individual still has an issue, then they may use the School's Grievance or Complaints Procedure.

14. AUDITS AND REVIEWS

The School will undertake regular internal audits of Boarding Houses and Departments to ensure this policy's requirements are being followed, including penetration testing.

This policy will be reviewed annually by the Privacy Officer in conjunction with the IT & Data Steering Committee and the Bursar's Management Group.

The School will publish on the website, or notify individually where necessary, any significant amendments to the provisions of this policy.

15. FUTURE PLANNING

The policy will be developed following issues raised by the internal audits, external audits and the internal reviews and in accordance with the law and regulation as it applies from time to time.

16. FURTHER INFORMATION

For further information concerning your rights as a data provider and our responsibilities as data processors and controllers, please see the privacy statement on the school website or the intranet.

17. CONTACT DETAILS

Privacy Officer: privacyofficer@harrowschool.org.uk

18. ADVICE LINES

Advice is also available from the Information Commissioner's Office at www.ico.gov.uk

Adopted by The Keepers and Governors of the Possessions, Revenues and Goods of the Free Grammar School of John Lyon within the town of Harrow on the Hill in the County of Middlesex on 17 September 2021.

Privacy Officer and the IT & Data Steering Committee

September 2021

Annual review

APPENDIX A – SUPPORTING POLICIES, PROCEDURES AND GUIDANCE

HS – (Parent and Pupil) Privacy Notice

HS – Staff Privacy Notice

HS – Staff ICT Acceptable Use Policy

HS – Archive Policy

HS – Photography Policy

HSEL – Photo Consent Policy

HA/HDT – Prospect Research Policy

HA/HDT – Data Handling Policy

APPENDIX B – DEFINITIONS

A. PERSONAL DATA

Personal data covers both facts and opinions about a living individual who can be identified from that data (or from that data and other information in the School's possession). It includes information necessary for employment such as the employee's name and address and details for payment of salary. It may also include information about the employee's health and appraisals at work.

B. PROCESSING OF PERSONAL DATA

Consent may be required for the processing of personal data unless the processing is necessary in accordance with the relevant lawful bases for the School to undertake its obligations to pupils, their parents or guardians, or staff.

The School collects the personal data it processes directly from the data subject and from third parties.

Any information which falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to parties with the consent of the appropriate individual or under the terms of this policy.

C. SPECIAL CATEGORIES OF PERSONAL DATA

The School may be required to process sensitive personal data regarding a member of staff. Where sensitive personal data is processed by the School, the explicit consent of the data subject or appropriate representative will generally be required in writing, although there are certain exemptions to this rule.

Sensitive personal data includes:

- medical information;
- racial or ethnic origins;
- political opinions or trade union membership;
- religious or other beliefs;
- offences committed or alleged;
- proceedings in respect of an offence and the disposal of such proceedings or sentence.

D. DATA CONTROLLERS AND DATA PROCESSORS

- *Processor* – means a person, public authority, agency or other body which processes personal data on behalf of the controller'.
- *Controller* – means the person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data'.

Processors are required to maintain a record of all categories of processing activities. This must include details of the controllers and any other processors and of any relevant Data Protection Officers, the categories of processing carried out, details of any transfers to third parties and a general description of technical and organisational security measures.

Processors are required to implement appropriate security measures such as encryption and the regular testing of effectiveness of any security measures. Data controllers and processors are also required under GDPR to notify the correct authorities of a data breach.

APPENDIX C – LIST OF INDIVIDUAL RIGHTS

- Right to information – to be informed about what personal data we process, how and on what basis (e.g. as set out in privacy notices).
- Right to access your own personal data by way of a subject access request.
- Correct any inaccuracies in your personal data.
- Right to request that we erase personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected.
- While requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, data subjects can apply for its use to be restricted while the application is made.
- Right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- Right to object if we process your personal data for the purposes of direct marketing.
- Right to receive a copy of your personal data and to transfer your personal data to another data controller.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- Right to be notified of a data security breach concerning your personal data if the breach is likely to result in a high risk to your rights and freedoms.
- Right to withdraw your consent (if the School is relying on consent to process the personal data).
- Right to complain to the Information Commissioner.

APPENDIX D – TYPES OF BREACHES

Confidentiality breach – where there is an unauthorised or accidental *disclosure* of, or *access* to, personal data.

Integrity breach – where there is an unauthorised or accidental *alteration* of personal data.

Availability breach – where there is an accidental or unauthorised *loss* of access to, or *destruction* of, personal data.