DATA PROTECTION POLICY

HARROW SCHOOL

INTRODUCTION

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

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 their duties and responsibilities. See Appendix A for a list of supporting policies, procedures and guidance.

You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

A list of the key definitions is included as Appendix B: Definitions.

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

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. It also applies to all officers of the School and breach of the policy may result in appropriate action being taken.

SCOPE

For the purposes of the 2018 Act, the School is the "data controller" of personal data. '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 within the town of Harrow on the Hill in the county of Middlesex.

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 adhere to this policy. This policy also covers staff and workers engaged by:

- Harrow School Enterprises Limited (HSEL)
- Harrow Association (HA)
- 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").

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.

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;
- everyone managing and handling personal data is appropriately trained to do so;
- everyone managing and handling personal data is appropriately supervised;
- anyone wanting to make enquiries about handling personal data, whether a member of staff or a member of the public, knows what to do;
- queries about handling personal data are promptly and courteously dealt with;
- methods of handling personal data are regularly assessed and evaluated;
- performance with handling personal data is 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, and any disclosure of personal data will be in compliance with approved procedures;
- conditions regarding the fair collection and use of personal data are observed in full;
- legal obligations to specify the purpose for which personal data is used are met;
- appropriate personal data, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements, is collected and processed;
- the quality of personal data used is ensured;
- retention procedures to determine the length of time personal data is held are applied;
- appropriate technical and organisational security measures to safeguard personal data are taken;
- ensure that personal data is not transferred abroad without suitable safeguards;
- 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, and meet its Data Protection by Design and Default obligations; and
- personal data must be processed in line with data subjects' rights.

ROLES AND RESPONSIBILITIES

The following roles and responsibilities apply:

Foundation IT Committee

Strategic accountability for the Corporation on IT and data-related governance.

IT Steering Committee

Strategic accountability for Harrow School/HSEL/HA/HDT on IT governance.

Data Management Committee

Operational oversight for Harrow School/HSEL/HA/HDT on IG (e.g. data protection, Freedom of Information and records management). Each department is represented on the committee. The departmental representative will, as part of their role:

- direct colleagues to guidance and provide support where possible; and
- identify and escalate issues and concerns to the Privacy Officer.

Privacy Officer

The School's Privacy Officer 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 this role by the Data Management Committee representatives and the committees outlined above.

All staff

All staff must comply with this policy and any related policies, procedures and guidance in order to meet duties and responsibilities.

PRIVACY INFORMATION AND FAIR 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 School will make accessible a Privacy Policy containing the further privacy information required by the Act.

The key Privacy Notices will be:

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

The Privacy Officer will maintain a list of Privacy Notices.

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 Public and Staff Photography and Film Policy, outlining the cases where it will rely on legitimate interests or consent to process photographs.

TRAINING

The Privacy Officer will arrange appropriate training for members of the Schools' staff and enforce the monitoring and review of this policy.

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 of all suppliers, consultants and partners who will handle (process) personal data on behalf of the School, and
- any contract or data sharing agreement 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.

HANDLING SUBJECT ACCESS REQUESTS (SARS) AND OTHER RIGHTS REQUESTS

Data subjects have a number of rights. 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; and
- have inaccurate data about them amended.

The full list can be found in Appendix C.

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
- compliant response can be provided.

Routine disclosures of personal data should be undertaken in accordance with agreed departmental procedures (see below).

ROUTINE DISCLOSURES AND USES OF PERSONAL DATA

School departments may need to share and access personal data to provide services or deliver their functions. The School may also 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, or 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 under the 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.

SECURITY OF PERSONAL DATA

All staff must adhere to the School's ICT policies:

- ICT Acceptable Use Policy
- Remote Working

All staff must adhere to the School's policies on:

- disclosing personal data over the phone;
- disclosing personal data via email; and
- storing paper records.

RECORDS RETENTION, DISPOSAL AND DATA ACCURACY

The School will endeavour to ensure that all personal data held in relation to data subjects is accurate.

- 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.

The School has 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.

DATA BREACH MANAGEMENT

The School must assess all breaches and decide whether it needs to report them to the Information Commissioner's Office (ICO) within 72 hours.

To ensure the School can meet this reporting deadline, all suspected or actual breaches must be reported immediately (as soon as you become aware of them) and keep any evidence you have in relation to the breach.

They must 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 Breach Handling Policy.

Examples of breaches can be found in Appendix D.

The School will follow the advice provided by the Information Commissioner's Office on how to manage data breaches and when to notify.

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.

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, before notifying 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.

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. Employees may use the School's Grievance Procedure.

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 Assistant Bursar, the ICT Steering Committee and the Bursar's Management Group.

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.

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's website or on Firefly.

CONTACT DETAILS

Privacy Officer:
Miss T R Fox
foxtr@harrowschool.org.uk
020 8872 8370

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 1 June 2019.

Privacy Officer
October 2019
Annual review

APPENDIX A: SUPPORTING POLICIES, PROCEDURES AND GUIDANCE

HS – Parent and Pupil Privacy Notice
HS – Staff Privacy Notice
HS – Job Applicant Privacy Notice
HS – IT Acceptable Use Policy
HS – Photography and Film Policy
HS – Subject Access Request Policy
HS – CCTV Acceptable Use Policy
HSEL – Photo Consent Policy
HA/HDT – Prospect Research Policy
HA/HDT – Data Handling Policy

APPENDIX B: DEFINITIONS

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.

PROCESSING OF PERSONAL DATA

Consent may be required for the processing of personal data unless the processing is necessary 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 third parties with the consent of the appropriate individual or under the terms of this policy.

SPECIAL CATEGORY 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; and
- proceedings in respect of an offence and the disposal of such proceedings or sentence.

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 for which it was collected.
- When requesting that your personal data is corrected or erased, or when 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.