AISL HARROW BEIJING 哈罗北京

HBJ DATA ACCESS & PROTECTION POLICY

APPLIES TO:	All staff, visitors, volunteers, contractors, governors, guests, residents
LAST UPDATED:	1st August 2024
REVISIONS: **(Reviewer to enter initials and date)**	PA – 28th February 2025

AISL HARROW BEIJING 哈罗北京

1 INTRODUCTION

1.1 AISL and its schools are fully committed to compliance with the principles of the data protection and access and will adhere to all local statute in this regard.

1.2 Each School will follow procedures that aim to ensure that 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, are fully aware of and abide by their duties and responsibilities under the local statute.

1.3 For the purposes of this Policy, the School is the "data controller" of personal data about students and their parents and/or guardians ("personal data").

2 STATEMENT OF POLICY

2.1 In order to operate safely and efficiently, each School has to collect and use personal data about people with whom it works.

2.2 This may include families of students, students themselves, members of the public, current, past and prospective employees, clients and customers, suppliers and other third parties. In addition, it may be required by law to collect and use personal data in order to comply with the requirements of government. This personal data must be handled and dealt with properly, however it is collected, recorded and used, and whether it be held on paper or electronically, regardless of media. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using personal data. In this Policy, any reference to students includes current, past or prospective students.

2.3 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 students, their parents or guardians, staff and those with whom it carries out business. To this end, the School fully endorses and adheres to the principles of Data Protection.

3 THE PRINCIPLES

3.1 The School shall, as far as is reasonably practicable, comply with eight Data Protection Principles, ensuring that all personal data processed by the School is:

- processed fairly and lawfully;
- obtained for specified purposes and only processed in accordance with those purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept for longer than necessary;
- processed in accordance with the data subject's rights;
- kept secure and protected.

4 PERSONAL DATA

4.1 Personal data cover 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.

4.2 The School may process a wide range of personal data of students, their parents or guardians as part of its operations. This personal data may include (but is not limited to) names, addresses, dates of birth, bank details, academic, disciplinary, admissions and attendance records, references, School reports, and examination scripts and marks.

5 PROCESSING OF PERSONAL DATA

5.1 Consent may be required for the processing of personal data unless the processing is necessary for the School to undertake its obligations to students, their parents or guardians, or staff.

5.2 The School collects the personal data it processes directly from the data subject (or, in the case of a student, her/his parents or guardians) and from third parties.

5.3 Any information that 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.

6 SENSITIVE PERSONAL DATA

6.1 The School may be required to process sensitive personal data regarding a member of staff or student, their parents or guardians. 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.

7 HANDLING OF PERSONAL DATA

7.1 The School will:

- observe in full local statues regarding the fair collection and use of personal data;
- meet its local legal obligations to specify the purpose for which personal data is used;
- collect and process appropriate personal data and only 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;
- ensure that personal data is not transferred abroad without suitable safeguards.
- publish for parents, information regarding its approach to data collection and processing via schedule 1 on the school's website.

7.2 The School will implement Privacy Impact Assessments (PIAs) in high-risk situations. PIAs are useful tools that help the School to consider and address the privacy risks involved in processing personal data. PIAs will be used when new projects or technology are deployed in the School to access and mitigate potential risk. PIAs should be used alongside existing project management and risk management methodologies. It is the responsibility of the project manager to consider potential risks and to contact the 'Privacy Officer', who is the nominated Deputy

Headmaster, with any concerns they may have. In the absence of the Executive Officer will act as the Privacy Officer.

7.3 Personal data must be processed in line with the data subjects' rights. Data subjects have a right to:

- request access to data about them held by the School (see paragraph nine of this Policy below);
- prevent processing in certain circumstances such as for direct marketing purposes or where the processing is likely to cause damage or distress to themselves or anyone else;
- ask to have inaccurate data about them amended.

8 PRIVACY OFFICER

8.1 The School's Privacy Officer will endeavour to ensure that personal data is processed in compliance with this policy.

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

9 RIGHTS OF ACCESS TO INFORMATION

9.1 Data subjects have a right of access to personal data about themselves held by the School. Any individuals wishing to access their personal data should put their request in writing to the Privacy Officer. The School will endeavour to respond to any such written requests within 30 working days. Administrative costs required to produce this data however must be born by the data subject. In many cases (for small requests) there will be no fee however for extensive requests, the administrative charges will be linked to reasonable time spent collating the information and associated printing costs.

9.2 A data subject can assist the School in responding to a data subject access request by specifying:

- the format of personal information being requested (e.g. hard copy documents or electronic communications);
- what the personal information relates to (e.g. education or pastoral care);
- the date or date range when the personal information was created.

9.3 The School will treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment of any student or employee. The School acknowledges that an individual may have the right to access a reference relating to them received by the School. Such a reference will only be disclosed if such disclosure will not identify the source of the reference, where the referee has given their consent, or if disclosure is reasonable in all the circumstances.

9.4 The School will, in most cases, rely on parental consent (or the consent of a guardian) to process data relating to students unless, given the nature of the processing in question and the student's age and understanding, it is unreasonable in all the circumstances to rely on the parent's (or guardian's) consent. The School will grant the student direct access to their personal data if, in the School's reasonable belief, the student understands the nature of the request. As a general guide, a child aged 12 or older is expected to be mature enough to understand the request they are making. A child may, however, be mature enough at an earlier age or may lack sufficient maturity until a later age and all requests will be considered on a case-by-case basis.

9.5 Where a student raises a concern confidentially with a member of staff and expressly withholds

their agreement to their personal data being disclosed to their parents or guardian, the School will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interest of the student or other students.

10 EXEMPTIONS

10.1 Certain data is exempted from the principles of Data Protection, including data in connection with or relevant to the following:

- the prevention or detection of crime;
- the assessment or collection of any tax or duty;
- where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School; and
- references given by the School.
- Where failure to share data could lead to the harm of a student

10.2 Data Protection principles also contain a number of exemptions when personal data may be withheld, including:

- personal data which might cause serious harm to the physical or mental health of the student or another individual;
- cases where the disclosure would reveal a child is at risk of abuse;
- personal data contained in adoption and parental order records;
- personal data given to a court in proceedings;
- copies of examination scripts;
- providing examination marks before they are officially announced.

10.3 The School will generally not be required to provide access to personal data held in an unstructured way. The School is also not required to disclose examination scripts to any student.

11 ACCURACY

11.1 The School will endeavour to ensure that all personal data held in relation to data subjects is accurate. Staff must notify the Human Resources department of any changes to personal data held about them, and students and their parents (or guardians) should contact Admissions.

11.2 An individual has the right to request that inaccurate personal data about them be erased or corrected.

12 DISCLOSURE OF INFORMATION

12.1 The School may receive requests from third parties to disclose personal data it holds about data subjects. The School confirms that it will not generally disclose information unless the individual has given their consent or where a specific exemption applies. The School does, however, intend to disclose such personal data as is necessary to third parties for the following purposes:

- to give a confidential reference relating to a student to any educational institution which it is proposed that the student may attend;
- to give a confidential reference relating to an employee;
- to give information relating to outstanding fees or payment history to any educational institution which it is proposed that the student may attend;
- to publish the results of public examinations or other achievements of students of the School;

- to disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips.

12.2 Where the School receives a disclosure request from a third party, it will take reasonable steps to verify the identity of that third party before making any disclosure.

13 THIRD PARTIES

13.1 The School may be required to pass personal data (including sensitive personal data where appropriate) to third parties on occasion. These third parties may process the School's data:

- to enable the relevant authorities to monitor the School's performance;
- to compile statistical information;
- to secure funding for the School or on behalf of individual students;
- to safeguard students' welfare and provide appropriate pastoral and medical care;
- where necessary in connection with learning and co-curricular activities undertaken by students;
- to enable students to take part in public examinations and other assessments and to monitor their progress and educational needs;
- to obtain appropriate professional advice and insurance for the School;
- where otherwise required by law;
- otherwise where reasonably necessary for the operation of the School and employment of its staff.

13.2 The School may also share personal data about International Old Harrovians (IOHs) with the Alumni Association, which may contact IOHs occasionally by post and email about the School and about AISL activities.

14 USE OF PERSONAL INFORMATION BY THE SCHOOL

14.1 The School will, from time to time, make use of personal data relating to data subjects in the following ways:

- to make use of photographic images of students or members of staff in School publications and on the School website;
- for fundraising, marketing or promotional purposes and to maintain relationships with students of the School, including transferring information to any association, society or club set up for the purpose of establishing or maintaining contact with students, or for development, fundraising, marketing or promotional purposes.

14.2 Should an individual wish to limit or object to any such use they should notify the Privacy Officer in writing.

15 DATA PROTECTION RESPONSIBILITIES

15.1 Day-to-day responsibility is undertaken by members of teaching and non-teaching staff. They will endeavour to ensure that all personal data is processed in compliance with the principles of good Data Protection. In addition, the School will ensure that:

- 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. Any disclosure of personal data will be in compliance with approved procedures.

15.2 All managers and staff in the School's departments will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and, in particular, will ensure that:

- paper files and other records or documents containing personal and/or sensitive data are kept in a secure environment;
- personal data held on computers and computer systems is protected by the use of secure passwords that, where possible, have forced changes periodically; and
- individual passwords are such that they are not easily compromised.

15.3 All contractors, consultants, partners or other agents of the School must:

- ensure that they and all their staff who have access to personal data held or processed for or on behalf of the School are aware of this Policy and are fully trained in and are aware of their duties and responsibilities.
- provide the School with information about how it processes data held on its behalf (if requested).

15.4 All contractors who are users of personal data supplied by the School will be required to confirm that they will abide by the requirements of data protection with regard to information supplied by the School.

16 ENFORCEMENT

16.1 If an individual believes that the School has not complied with this policy, he or she should notify the School's Privacy Officer or an appropriate Senior Manager. Employees may use the School's Grievance Procedure. Students and parents (or guardians) may use the External Complaints Procedure.

17 DATA BREACH MANAGEMENT

17.1 In the event of a suspected breach of data protection, the following will be addressed by the School:

- containment and recovery;
- assessment of ongoing risk;
- notification of breach;
- evaluation of response.

17.2 If an individual believes that the School has not complied with this Policy, the individual should notify the Privacy Officer who shall, where appropriate, refer the matter for resolution in accordance with the School's grievance/disciplinary procedure (for staff) or complaints procedure (for parents/students).

17.3 This Policy forms part of the terms and conditions of all employee's 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.

18 AUDITS

18.1 The School will undertake regular internal audits of academic and administrative departments, and boarding houses if operated by the School, to ensure this Policy's requirements are being followed, including penetration testing.

19 REVIEWS

19.1 This Policy will be reviewed annually by the Privacy Officer in conjunction with the Director of Operations, the ICT Steering Committee and the Board of Governors.