Habs

HABERDASHERS'
ELSTREE SCHOOLS

Data Protection Policy

Policy Type	Statutory
Regulation	Data Protection Act 2018 General Data Protection Regulations 2018
Approval Committee	Risk Management and Compliance Committee
Last Review	Summer 2023
Next Review	Summer 2024

1 Related Information 3
1.1 Availability of Statutory Policies 3
1.2 Statutory Guidance 3
1.3 Supporting Documents 3
1.4 Terminology 3
2 Introduction 4
3 Key Principles of GDPR 5
4 Lawful Grounds of Data Processing 5
5 Types of Personal Data Processed by the School 6
5.1 Examples of places where Personal Data might be found are: 6
5.2 Examples of documents where Personal Data might be found are; 6
6 Sharing Personal Data 7
7 Personal Data must not be kept for longer than necessary 8
8 Record Keeping 8
9 Avoiding, mitigating and reporting data breaches 8
10 Rights of Individuals 9
11 Requests for Personal Data (Subject Access Requests) 9
12 Data Security: online and digital 10
13 Processing of Financial / Credit Card Data 11
14 Audit and Review 11

1 Related Information

1.1 Availability of Statutory Policies

All statutory policies are available on the School's website.

1.2 Statutory Guidance

This statutory policy has been reviewed in accordance with the following guidance:

Data Protection Act 1998 2018 General Data Protection Regulations 2018

1.3 Supporting Documents

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

CCTV Policy
Data Breach Policy
Acceptable Use Policy - Staff
Acceptable Use Policy - Students
Information Security Management Policy
Privacy Notice for Staff
Privacy Notice for Parents
Privacy Notice for Parents of Younger Students
Privacy Notice for Older Students
Retention of Data and Erasure of Personal Information Policy
Safeguarding Policy
Subject Access Request Policy
Taking, Storing and Using Images of Students'

1.4 Terminology

Data controller - a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its trustees / governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

Data processor - an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

Data Subject means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

GDPR means General Data Protection Regulations.

Parents includes one or both parents, a legal guardian, or education guardian.

Personal information (or personal data) - any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

School means Haberdashers' Aske's Elstree Schools Limited as Trustee of Haberdashers' Aske's Charity trading as Haberdashers' Girls' School **and/or** Haberdashers' Boys' School, as now or in the future constituted (and any successor).

Special Categories of personal data (also known as sensitive personal data) – relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health and medical conditions, sex life or sexual orientation used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences. Staff must be particularly careful when dealing with Personal Data which falls into any of these categories.

Student or **Students** means any Student or Students in the School at any age.

2 Introduction

This policy applies to all staff working in the School (whether directly or indirectly), whether paid or unpaid whatever their position, role or responsibilities which includes employees, Governors, contractors, agency staff, work experience / placement students and volunteers. This Policy is about your obligations under the data protection legislation.

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, students, employees, contractors and third parties). It also gives people various rights regarding their data, such as the right to access the Personal Data the School holds on them.

Those who handle personal data as employees or Governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

3 Key Principles of GDPR

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

- Processed fairly, lawfully and in a transparent manner
- Collected for specific and explicit and only for the purposes it was collected for
- Relevant and limited to what for the purposes it is processed
- Accurate and kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed, and
- Processed in a manner that ensures appropriate security of the Personal Data.

The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- Keeping records of our data processing activities, including by way of logs and policies
- Documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- Generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

4 Lawful Grounds of Data Processing

Under the GDPR, there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible. One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires. Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

5 Types of Personal Data Processed by the School

The School may process a wide range of personal data about individuals including current, past and prospective student, their parents, governors and employees as part of its routine operations including:

- names, addresses, telephone numbers, e-mail addresses and other contact details
- car details (about those who use School car parking facilities)
- bank details and other financial information, e.g. about parents who pay fees to the School or payroll details for members of staff
- past, present and prospective students' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks
- where appropriate, information about individuals' health, and contact details for their next of kin
- references given or received by the School about students, and information provided by previous educational establishments and / or other professionals or organisations working with students as well as references supplied by previous employers of staff
- academic and professional qualifications as well as relevant previous experience and annual reviews of employees
- images of students (and other individuals) engaging in School activities, and images captured by the School's CCTV system (and the policy on taking, storing and using images of children).

Generally, the School receives personal data from the individual directly (or, in the case of students, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual) or collected from publicly available resources.

5.1 Examples of places where Personal Data might be found are:

- On a computer database
- In a file, such as a student report
- A register or contract of employment
- Students' exercise books, coursework and mark books
- Health records
- Email correspondence

5.2 Examples of documents where Personal Data might be found are;

- A report about a safeguarding incident
- A record about disciplinary action taken against a member of staff
- Photographs of students
- Contact details and other personal information held about students, parents, staff and their families
- Contact details of a member of the public who is enquiring about placing their child at the School
- Financial records of a parent
- Information on a student's performance; or
- An opinion about a parent or colleague in an email.

This list is not exhaustive, there may be many other processes that would use Personal Data.

Particular care must be taken when dealing with Personal Data which fall into any of the Special Categories below:

- Information concerning safeguarding matters.
- Information about confidential medical conditions and information about educational learning needs.
- Information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved).
- Financial information (for example about parents and staff).
- Information about an individual's racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- Genetic information.
- Information relating to actual or alleged criminal activity.
- Biometric information (e.g. student's fingerprints).

Any concerns about the processing of these Special Categories of Personal Data, should be raised with the Chief Operating Officer (COO).

6 Sharing Personal Data

The School will not normally share personal data with anyone else without consent, but there are certain circumstances where this may be required. These include, but are not limited to situations where:

- There is an issue with a student or parent/carer that puts the safety of staff at risk
- There is a need to liaise with other agencies
- Trust suppliers or contractors need data to enable services to be provided.

When doing this, the School will:

- Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data being shared
- Only share data that the supplier or contractor needs to carry out their service.

Personal data is shared with law enforcement and government bodies where the School is legally required to do so.

The School will also share personal data with emergency services and local authorities to help them to respond to an emergency situation.

If the School is required to transfer personal data internationally, this will be done in accordance with UK data protection law.

It should be noted, from the outset, that data protection should always take second place to safeguarding and child protection. If there is potential conflict between these competing requirements, the welfare of the child is paramount.

The COO is responsible for helping the School to comply with the School's obligations. All queries concerning data protection matters should be raised with him.

7 Personal Data must not be kept for longer than necessary

The School has an Retention of Data and Erasure of Personal Information Policy which contains details about how long different types of data should be kept and when records should be destroyed. This applies to both paper and electronic documents. Care needs to be taken especially when deleting data.

8 Record Keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *any* personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, students and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or students, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

9 Avoiding, mitigating and reporting data breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in the Data Breach Policy.

One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach, they must notify the COO. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

10 Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School).

Individuals have legal rights to:

- obtain access to, and copies of, the personal data that are hold about them
- require the School to correct the personal data held about them if it is inaccurate
- request that the School erase their personal data (in certain circumstances)
- request that the School restrict its data processing activities ((and, where processing is based on the individual's consent, they may withdraw that consent, without affecting the lawfulness of processing based on consent before its withdrawal)
- receive from the School the personal data it holds about an individual for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention)
- object to direct marketing; and,
- withdraw one's consent where the School relies on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

11 Requests for Personal Data (Subject Access Requests)

One of the most commonly exercised rights is the right to make a Subject Access Request (SAR). Under this right people are entitled to request a copy of the Personal Data which the School holds about them (or in some cases their child) and to certain supplemental information. Receiving a SAR involves complex legal rights. Staff must never respond to a SAR themselves without consulting the COO.

Personal data about a student belongs to that student, and not the student's parents or carers. For a parent or carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR or have given their consent. Children's rights under the GDPR is explained in more detail.

Students below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of students at Prep/Junior School may be granted without the express permission of the student. This is not a rule and an individual's ability to understand their rights will always be judged on a case-by-case basis.

Students aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of students may not be granted without the express permission of the student. This is not a rule and an individual's ability to understand their rights will always be judged on a case-by-case basis.

Please note that the above rights are not absolute, and the School may be entitled to refuse requests where exceptions apply. Information should not be disclosed if it:

- might cause serious harm to the physical or mental health of the student or another individual
- would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- would include another person's personal data that cannot reasonably be anonymised, the other person has not provided consent and it would be unreasonable to proceed without it
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- is a request that is unfounded or excessive, the School may refuse to act on it, or charge a reasonable fee to cover administrative costs. The School will take into account whether the request is repetitive in nature when making this decision; and,
- when a request is refused, the individual will be told why, and informed that they have the right to complain to the ICO.

The School will endeavour to respond to any such requests as soon as is reasonably practicable and in any event within statutory time-limits (which is generally one month, but actually fulfilling more complex or multiple requests, e.g. those involving third party information, may take 1-2 months longer).

In any event, however, if a request is received from an individual who is purporting to exercise one or more of their data protection rights, the COO must be informed as soon as possible.

12 Data Security: online and digital

More generally, all School staff and contractors are expected to remain mindful of the data protection principles (see section 2 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

It is expected that all those with management / leadership responsibilities be particular champions of these principles and to oversee the swift reporting of any concerns about how

personal information is used by the School to the COO and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. With reference to Acceptable Use Policy – Staff:

- No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the COO
- No member of staff should provide personal data of students or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so
- Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.
- Use of personal email accounts or personal devices by Governors or staff for official School business must be password protected.

13 Processing of Financial / Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. Further guidance can be sought from the Director of Finance and Resources. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

14 Audit and Review

To ensure compliance with the latest data protection legislation, the School will undertake periodic audits of systems and business processes to identify areas of non-compliance or improvement.

This policy will be reviewed periodically and updated in accordance with changes in legislation.