HIGHGATE WOOD SCHOOL

Data Protection Policy

2018

Ratified by the Governors Finance Committee: 23 May 2018
This Policy is due for review May 2020 (Every 2 years)

'**Making a positive difference** to students' achievements and experiences, maintaining the **highest expectations** and inspiring **self-belief**'

Everyone Matters

Contents

Introduction

Highgate Wood School collects and uses personal information about students, staff, parents, governors and others who come into contact with the school. The information is gathered in order to enable the school to provide a public education service and associated functions. In addition there is a legal requirement for us to handle information to comply with our statutory obligations.

The school is committed to ensuring the privacy and security of the personal data that it collects, stores and processes and that all operations are carried out in accordance with the General Data Protection Regulation (GDPR) and other associated and relevant legislation.

This policy provides the framework through which the school's data processes operate. The policy applies to all personal data handled, regardless of whether it is in paper or electronic format.

Legislation and Guidance

This policy has been based on the guidance published by the Information Commissioner's Office (ICO) and by other guidance that is referenced on the ICO website (https://ico.org.uk)

The school's use of personal data, what data is collected and stored and with whom it is shared, is explained in the Privacy Notices that are available on the school website as well as appendixes to this policy.

If you have any enquiries in relation to this policy please contact the schools Data Protection Officer at dataprotection@hws.haringey.sch.uk

Further advice and information regarding data protection and the obligations of schools in relation to personal data are available from the Information Commissioner's Office at www.ico.gov.uk.

The data controller

Highgate Wood School processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO (Registration reference: **ZA093721**) and will renew this registration as legally required to do so.

Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Our DPO is Tristan Ashman and is contactable via dataprotection@hws.haringey.sch.uk

Headteacher
The Headteacher acts as the representative of the data controller on a day-to-day basis.

All staff (including governors*)*
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Ensuring their practice minimise any risks to the integrity of personal data held by the school and helps ensure the continued privacy and protection of data subjects
- Informing the school of any changes to their own personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If there has been a data breach
    - Before engaging in a new activity that may affect the privacy rights of individuals

Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

Collecting personal data

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** or take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of an individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. The information that we collect, hold and share, the reasons why we collect and use this information and the lawful basis for us to collect this information are explained in our Privacy Notices.

Our procedures for retention of personal data are outlined in our Record Management Policy which is informed by the Information and Records Management Society's toolkit for schools.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff or students at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, companies that provide online services to students and\or their parents.

When doing this, we will:

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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

Overview

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the personal data held
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. If another member of staff receives a subject access request they should forward it to the DPO.

Children and subject access requests

Children at secondary school are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we may ask for further information to confirm the identification of the person making the request and to ensure that the nature of the request is fully understood.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Breach the data privacy rights of another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the Information Commissioner's Office.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see our Privacy Notices), individuals have the right to:

- Where the legal grounds for collecting personal data is consent that consent can be withdrawn at any time
- Ask us to rectify, update or amend any personal data that we hold that is inaccurate or out of date.
- In certain circumstances require us to erase or restrict processing of their personal data, or object to the processing of it
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area if this practice occurs
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they should immediately forward it to the DPO.

Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

In accordance with the principles of GDPR and the privacy of all our data subjects any information on a school record that identifies another data subject and risks that data subject's privacy will be redacted before the educational record is released.

Biometric recognition systems

Highgate Wood School is always considering ways in which we can improve our facilities and efficiency. It may be that we will wish to make use students' biometric data as part of an automated biometric recognition system (for example, students using finger prints to pay for school meals rather than using cards). If this is the case we will ensure our plans comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is implemented and appropriate systems of consent will be put in place. Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Steve Hatch, the school's Business Manager at shh@hws.haringey.sch.uk.

Photographs and videos

As part of our school activities, we may take – or arrange to have taken - photographs and videos of individuals within our school for communication, marketing and promotional materials.

For students who are under the age of 16 we request written consent from parents/carers and students at the time of joining the school. For students aged 16 and over we request their consent alone.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

When using photographs and videos in this way we will not accompany them with any other personal information about the child if the student is under the age of 16, to ensure they cannot be identified. For students over the age of 16 we would not ordinarily have any other identifiers but should there be an occasion when the post-16 student is identified (e.g. with their name and university destination on the "Wall of Fame") explicit consent is requested and recorded.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Data protection by design and default

We endeavour to integrate data protection into all our data processing activities and achieve this by a number of different means, including:

- Completing and maintaining an Information Asset Register and a Risk Assessment Register for the school's systems and procedures for entering, storing and sharing information
- Only processing personal data in line with the principles set out by relevant data protection law
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters
- Providing regular reminders to staff of the importance of data security and data privacy and how to help ensure this
- Promoting a culture of vigilance and awareness around the risks of personal data being unwittingly shared
- Regularly conducting reviews and audits to test our privacy measures

- Maintaining records of our processing activities, including:

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular **staff** are advised that:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data must be kept secure when not in use
- Papers containing confidential personal data must not be left on view on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords to the school network are complex alphanumeric for greater security and staff are reminded to change their passwords at regular intervals.
- Separate passwords are required to access the school's management information system, Sims.net, where most of the more sensitive personal data is stored.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use Policies and our Digital Safety Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours and\or inform those who may be affected or impacted by the suspected data breach.

Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

Links with other policies

This data protection policy is linked to our:

- Freedom of information Policy
- Record Management Policy
- Digital Safety Policy
- Acceptable Use Agreements
- Data Breach Procedures (Appendix 1)
- Privacy Notices (Appendix 2

Appendix 1: Personal Data Breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding, suspecting or causing a breach, or potential breach, the member of staff (or other individual) should immediately notify the DPO (dataprotection@hws.haringey.sch.uk). The DPO will investigate the report, and determine whether a breach has occurred. The DPO will consider whether personal data has been accidentally or unlawfully:

- Lost or Stolen
- Destroyed or Altered
- Disclosed or made available where or to whom it should not have been
- Made available to unauthorized people.

When a personal data breach has occurred, the DPO will make all reasonable efforts to contain and minimize the impact of the breach, assisted by relevant staff members or data processors where necessary.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen. The DPO will focus on the potential negative consequences as explained in Recital 85 of the GDPR.

If it is judged likely that there will be a risk to an individual's rights and freedoms then the school will notify the ICO; if it is judged unlikely to be a risk to an individual's rights and freedoms then the breach will be documented and reported to the Headteacher with a justification of why an ICO report was not made.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours and submit the information that is required. If all the details are not yet known, the DPO will report as much as they can within 72 hours. The DPO will submit the remaining information as soon as possible having already explained the reasons for the delay.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

The name and contact details of the DPO

A description of the likely consequences of the personal data breach

A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. These reports will follow the guidelines laid down by the Information Commissioner's Office