HALL GREEN SCHOOL

DATA PROTECTION POLICY

Adopted:	8 February 2023
Next Review:	February 2025
Governing Committee:	Full Governing Body
Responsibility:	Headteacher
	Chair of Governors

Policy Objectives

UK General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. Hall Green School as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

Scope and principles

According to Article 2(a) of the GDPR, "personal data" is defined as "any information relating to an identified or identifiable natural person ("data subject!"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". As a consequence, any information containing two or more of the following would be classified as personal data:

- Religion
- Ethnicity
- FSM status
- Name
- Date of Birth
- Photographs of the data subject
- Address
- Parental contact information
- UPN (Unique Pupil Number)
- Medical information – e.g. disabilities
- Form group information/class information
- Assessment information
- Anything else that could cause embarrassment to a child or parent or bring the school's good name into disrepute.

Separate consent is obtained for the use of biometric data, which is classified as "sensitive personal data". Biometric data is used by Chartwells, our catering company, to provide an alternative method of identifying pupils and staff when purchasing items.

The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Individual rights

The GDPR provides the following rights for individuals (data subjects):

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

For further information, please visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights. Privacy notices are available for parents/carers, pupils, staff/trustees/governors/volunteers and visitors at http://www.hallgreen.bham.sch.uk/policies.

Article 6(1)(c) provides a lawful basis for processing where "processing is necessary for compliance with a legal obligation to which the controller is subject". In circumstances such as the census, this applies. In all other cases where data processed would not be required legally, the home/school agreement constitutes consent to process this data.

Transfer Limitation

In addition, personal data shall not be transferred to any country unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data or where the organisation receiving the data has provided adequate safeguards.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the UK.

Information Security

Hall Green School will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested

Storage and retention of personal information

Personal data will be kept securely in accordance with the school's data protection obligations, and should not be retained for any longer than necessary. Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. As a consequence, Hall Green School use the following retention and deletion schedule:

Pupil data- Main pupil record

Record type	Retention period
Record of transfer from Early Years setting	No more than nine years after pupil departs
Admission Form	No more than nine years after pupil departs
Data Collection/Checking Form	No more than nine years after pupil departs

Annual written report to parent(s)/carer(s)	No more than nine years after pupil departs
National Curriculum and Religious Education locally agreed syllabus record sheets	No more than nine years after pupil departs
Any information relating to a major incident involving the child	No more than nine years after pupil departs
Statements/Plans, reports, etc. for educational support, e.g. SEN, Speech and Language	No more than nine years after pupil departs
Medical information relevant to the child's on-going education/behaviour	No more than nine years after pupil departs
Child protection reports/disclosures and supporting documentation	No more than nine years after pupil departs
Any information relating to exclusions (fixed or permanent)	No more than nine years after pupil departs
Specific correspondence with parents or outside agencies relating to major issues	No more than nine years after pupil departs
Summary details of complaints made by the parents or the pupil relevant to the child's on-going education/ behaviour	No more than nine years after pupil departs
Examination Results – pupil copy	No more than nine years after pupil departs
SATS Results	No more than nine years after pupil departs
The following record types are stored separately to the main pupil record, and are subject to the retention periods outlined in the 2019 IRMS Toolkit for School (https://irms.org.uk/page/SchoolsToolkit)	
Attendance Registers and Information	
Absence (authorised) notes and correspondence	
Parental consent forms for trips/outings	
Accident forms (a copy can be placed on the pupil record if it is a major incident)	
Medical consent and administering records (this is the school's record)	
Copies of birth certificates, passports, etc.	
Generic correspondence with parents about minor issues (i.e. 'Dear Parent')	
Pupil work, drawings, etc.	
Previous data collection forms which have been superseded (there is no need to retain these)	
Photography (image) consents (this is the school's record)	
Pupil photographs	

In the event of a particular data type falling outside of the above specified criteria, Hall Green School will decide upon a retention period befitting the sensitivity, risk and any possible legislation.

In regards to staff data, retention information is also subject to the retention periods outlined in the 2019 IRMS Toolkit for Schools (https://irms.org.uk/page/SchoolsToolkit).

Use of external organisations

Where Hall Green School uses external organisations to process personal information on its behalf, contracts with those organisations will be in place before any process is undertaken in order to safeguard the security of the subject's personal data. Contracts will ensure that:

- the organisation may only act on the written instructions of the school;

- those processing data are subject to the duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the school and under a written contract;
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will delete or return all personal information to the school as requested at the end of the contract;
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Demonstrating compliance: Organisational protocols

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles". As an organisation, Hall Green School ensure that in order to fully comply with GDPR, and further to any obligations already mentioned, the following additional processes will also be followed:

- We will ensure comprehensive whole-school staff training, internal audits of processing activities and reviews of internal HR policies.

- We will implement measures that meet the principles of data protection by design and data protection by default. Where possible, data minimisation, pseudonymisation and transparency are employed.

- We will create, apply and improve security features on an ongoing basis.

- We use data protection impact assessments. This means that before any proposed data-processing agreement is finalised, an internal assessment must take place where the DPO and any other relevant parties discuss details and log the outcome and decision.

Demonstrating compliance: Staff protocols

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy. The Information Commissioner as the Regulator can impose fines of up to £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher, for serious breaches of the GDPR, therefore it is imperative that the School and all staff comply with the legislation.

As an individual member of staff, you have a personal responsibility to act in a professional way to maintain the integrity of data and engage in all of these organisational protocols implemented by Hall Green School as they relate to our obligation to comply with GDPR and uphold the rights of

any data subject(s). For all members of staff, the following personal directives must also be adhered to:

When storing or working with data

- Only store pupil data on school equipment, e.g. network drives (staff area, staff shared area etc.). Only school-issued encrypted USB devices are permitted. **Any member of staff using a personal USB device as opposed to a school-issued USB device may be subject to disciplinary procedures.**

- Staff must not routinely take pupil data off-site if it contains sensitive information that could either identify a pupil or cause embarrassment if the data was lost/seen by another individual. In cases where staff feel this is unavoidable, please see the SIRO. Marking of books or pupil work should not be considered a risk, provided extraneous pupil data is not present.

- Staff are responsible for destroying their own data once it is **no longer required.** This should be immediately after the "event" or at the end of the academic year if it is required for a longer period of time. Pupil coursework can be destroyed once certification is obtained, but may be retained for longer if staff feel this is necessary. If this is the case, the individual retaining it is personally responsible for secure storage and destruction before the pupil in question is twenty-five years of age (no longer than nine years after the pupil leaves school).

- Diaries that contain notes from meetings etc. that identify pupils or staff should be stored securely when not in use.

- When socialising do not discuss any individuals from work as you are never fully aware of who is listening.

- Never send personal information regarding pupils or staff via pupils.

- Staff must take every precaution to ensure they do not display potentially personal/sensitive data on smartboards or in visible documents. SIMS/Class Charts/e-mail should not have pupil or staff details "broadcasting" to pupils, if those details could cause undue distress, alarm or embarrassment. It is perfectly reasonable to have the register document open in SIMS, the seating plan (without personal data) on Class Charts or any other information with generally "known" information.

- In cases where information regarding pupils, parents or staff would be sent via email, you should consider whether the content could significantly compromise the data subject if read by another party. For example, details regarding bereavement, health, special needs or safeguarding concerns should be password protected within a word document.

- If using social media, you are advised to use a screen name, do not accept students as 'friends', and do not discuss work-related personal data.

When communicating within and outside of Hall Green School

- You must take personal responsibility for checking email addresses/groups/contact details if you are sharing personal or sensitive data. **Any data breaches attributed to entering incorrect details are the responsibility of the individual.**

- When communicating with any individual, staff must always use professional and appropriate language. Remember that all communications could be the subject of a Freedom of Information request, and thus become a public document if the data subject chooses.

- In cases where an email contains personal data which should be retained on record (see retention schedule above), staff must write a note or complete a report in SIMS and then should delete the email.

- It is advised that you delete/empty email trash every 3 months. In the event of an investigation, records of all kinds are called for and staff are personally responsible for the ongoing maintenance of their school email accounts

- All electronic communications with pupils and parents must be through school email addresses, texting services and the official School Twitter account. When contacting pupils, it is only permitted to email their school email address, not a pupil's personal email address.

- Staff must ensure adequate and appropriate security measures are taken when accessing email/pupil data/work-related content from personal devices such as mobile phones, tablets, laptops and personal computers. Accounts should always require a password to be entered, and should not be automatically saved (auto-login).

- When printing and distributing data subject information, this should only be relevant for the purpose, should not contain extraneous information and the number printed should not exceed the number required.

- Do not leave computers or electronic devices unlocked and unattended in a classroom, if they contain personal data. Keyboards must be locked and screens must not be showing personal data. If an offence is committed by a third-party whilst a device is logged in, the person whose login is used is also responsible even if they do not commit the offence.

- Do not take or store photos of pupils on personal devices.

- If a third-party wishes to use images/footage of our pupils, they must obtain consent themselves. Our consent record only applies to our own use (Twitter/website/promotional material etc.). It DOES NOT mean third-parties can assume consent. They MUST obtain separate written permission (usually through their own consent form)

- You must check the updated photographic consent permissions list before using pupil photographs for school-related purposes.

- Records of assessment or meetings must be securely disposed of once the work is no longer needed.

- ROA reports must be spell-checked and proof-read to minimise data inaccuracy.

- Trip documentation should be destroyed once you are confident that the trip occurred without incident. If an incident has occurred documents must be submitted to the Trips Organiser and will be kept for 25 years. If unsure, you must speak to the Trips Organiser or Headteacher immediately upon your return.

- Information on walls in offices/classrooms where parents may be taken for meetings must be covered up or removed before the meeting is held.

Information Loss/data breach Process

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information either by a member of staff or third party;
- Loss of data resulting from an equipment or systems (including hardware or software) failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as a fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams;
- Blagging offences where information is obtained by deceiving the organisation which holds it.

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform the DPO immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process. In cases where a member of staff has become aware that a potential information loss has occurred, they must report the loss immediately to the Data Protection Officer (DPO). Regardless of circumstances, reporting must occur within **72 hours.**

The reporting process will involve:

- discussing the nature of the data;
- the potential implications of the loss;
- the potential need to inform parents, the police or the Information Commissioner;
- determining if disciplinary action is required due to negligence.

Staff should be aware that data breaches resulting from a deliberate or grossly negligent failure to adhere to the personal responsibilities under the school data protection protocol could result in disciplinary procedures. In any case when the act of negligence is significant enough to warrant the involvement of the Information Commissioner or potential legal proceedings, Hall Green School will fully support any external enquiry.

Privacy Notices

The school issues and publicises privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes. Privacy notices are currently available at https://www.hallgreen.bham.sch.uk/policies/.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data). When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language, issue a minimum of two privacy notices, one for pupil information, and one for workforce information and these will be reviewed in line with any statutory or contractual changes.

Review of Policy

If necessary, this policy will be updated to reflect statutory amendments made to GDPR or DPA before the upcoming review date. Failing any updates or amendments, this policy will be reviewed after two years.

Data Protection Officer (DPO)

Designated DPO for Hall Green School is Mr Stephen Ancell.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.