THE HALL SCHOOL

DATA PROTECTION POLICY

AUTHOR: Varsha Patel

Policy ratified by: SLT

Date of last publication: September 2021
Date of next review: September 2022

Registered with the ICO as a Data Controller and Processor: Registration Number: Z8203376

This policy is available on the School website and can be made available in large print or other accessible format if required.

AIMS OF THE DATA PROTECTION POLICY

The Hall aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed, in accordance with the The General Data Protection Regulation (GDPR) 2018.

The General Data Protection Regulation (GDPR) is a European Commission Regulation intended to strengthen and unify data protection for individuals within the European Union (EU). The Commission's primary objectives of the GDPR are "to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU". The EU Council and the Parliament both adopted the regulation in April 2016. The regulation is effective from 25 May 2018. On 14 September 2017, the UK Data Protection Bill was published. This replaced the Data Protection Act (DPA) 1998 and incorporate the GDPR into UK legislation.

This policy sets out how the school seeks to protect personal data and ensure that staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

This policy is intended to provide information on the school's use of personal data about individuals including current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents"), staff and visitors. It should be read in conjunction with the school's other policies relating to internet and email use, IT security, Privacy Policy, Retention of Records Policy and all other data related policies.

Anyone who works for, or acts on behalf of, the school (including staff, volunteers, governors and service providers) should also be aware of and comply with this data protection policy, as well as the Privacy Notices.

DEFINITIONS	
Data subject	The natural person whose personal data is held or processed.
Types of data/data subjects	Administrative: pupil, parent (current and prospective) and staff. Personnel: Staff, payroll and regulatory Financial: Staff, parents and suppliers Regulatory: Ofsted, ISI, D of E, Charity Commission Marketing & fundraising: Alumni, parents
Business Purposes	The purposes for which personal data may be used by us:
	Compliance with our legal, regulatory and corporate governance obligations and good practice.
	Operational reasons.
	Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments. Monitoring staff conduct, disciplinary matters.
	Marketing our business and improving services
	Ensuring business policies are adhered to (such as policies covering email and internet use).
	Investigating complaints.
Personal Data	Personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one 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.
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Examples of data collected	Examples of Personal Data we collect: Email address; home address; phone number; bank details; national insurance number; medical details; references; nationality and educational background.
Data Controller	Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

DEFINITIONS (CONTINUED)	
Data Processor	Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory Authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

THE HALL AS A DATA CONTROLLER
The Hall collects data and determines the purpose and the means of processing personal information relating to pupils, staff and visitors, and, therefore, is a data controller. The Hall school is registered as a data controller and processor with the Information Commissioner's Office and renews this registration annually. Registration Number: Z8203376.
DATA PROTECTION OFFICER
The Data Protection Officer 'DPO' is responsible for co-ordinating the School's Data Protection systems and policies. All requests from data subjects regarding their data should be referred to the DPO. All data breaches should be reported to the Headmaster and DPO.

SCOPE
This policy applies to all staff and other authorised third parties (including temporary and agency workers, contractors, interns and volunteers) who must be familiar with this policy and comply with its terms.
The information covered by this policy includes all written, spoken and electronic personal data held, used or transmitted by or on behalf of The Hall in whatever media. This includes personal data held on computer systems, hand held devices, phones, paper records and personal data transmitted orally.
This policy supplements our other policies relating to internet and email use, IT security, Privacy Policy , Retention of Records Policy and all other data related policies.
We will review and update this policy in accordance with our data protection obligations We may amend, update or supplement it from time to time and will issue an appropriate notification at the relevant time

PRINCIPLES OF DATA PROTECTION	
The Hall will comply with the following principles of data protection under the provisions in the EU General Data Protection Regulation. The Principles are that data collection must be:	
1. **Lawful, fair and transparent**	Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used. *Details are set out in the privacy policy for pupils, parents and staff.*
2. **Limited for its purpose**	Data may only be collected for a specific purpose.*eg. to fundraise or to complete the parent contract.*
3. **Data minimised**	Any data collected must be necessary and not excessive for its purpose. *Always set out requesting* the minimum data and frequently review whether its retention is necessary.
4. **Accurate**	Any data we hold must be accurate and kept up to date. *Refresh parents and staff data termly*
5. **Retained Correctly**	Data should not be stored for longer than necessary. *Use the retention policy and enforce it strictly.*
6. **Storage**	Data must be held safely and securely. Lock filing cabinets, *use passwords and close the computer when leaving your office . keep personal devices secure.*

PROCEDURES
The Hall must demonstrate that the school complies with each Principle
Staff who collect data on behalf of the school are responsible for keeping a written record of use of data and for understanding their responsibilities to ensure compliance with each of the Principles. This must be kept up to date and must be approved by the DPO
ACCOUNTABILITY AND TRANSPARENCY
The Hall and its staff must ensure accountability and transparency in all the use of personal data. This should be demonstrable to data subjects through the documentation of the measures, both technical and organisational, which have been established in order to comply with the requirements of the GDPR. The Privacy policy should be available to all data subjects to ensure that there is the required transparency the use of their data.
FAIR AND LAWFUL PROCESSING
The Hall must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle.
This generally means that personal data should t not be processed unless the data subject has the authority to consent and has consented to this happening. If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful
Data subjects have the right to have any data unlawfully processed erased.

LAWFUL BASIS FOR PROCESSING DATA		
The six lawful bases for processing data are set out below. The Hall's privacy notice states that it regards its lawful basis for processing data is by use of a contract and the pursuit of legitimate interest.		
Any data for which staff are responsible for managing must be processed under the above bases. The DPO will regularly review and approve these bases. Staff who are working with data must refer to the lawful basis before processing that data and check that all of their actions comply the lawful basis.		
At least one of the following conditions must apply whenever we process personal data		
More than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.		
	CONDITION	**(One of the following must apply in order to process personal data)**
LAWFUL BASES FOR THE HALL		
1	**Legitimate Interest**	The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.
2	**Contract**	The processing is necessary to fulfil or prepare a contract for the individual
OTHER LAWFUL BASES AVAILABLEIN THE LEGISLATION		
3	**Consent**	We hold recent clear explicit and defined consent for the individuals data to be processed for a specific purpose
4	**Legal obligation**	We have a legal obligation to process the data
5	**Vital Interest**	Processing the data is necessary to protect a person's life or in a medical situation
6	**Public Function**	Necessary to carry out a task of public interest or a function which has clear basis in law
ASSESSING THE LAWFUL BASIS FOR PROCESSING		
In order to assess the lawful basis for processing, staff must first establish that it is necessary; the processing must be a targeted, appropriate way of achieving the stated purpose. Staff must examine and document the lawful basis for each processes which the DPO must approve .The Privacy notice should describe this approach.		

FACTORS TO CONSIDER	
Purpose:	Could the objective be achieved without collecting data or using a different approach.
Data subject:	Would The Hall's legal basis for processing data correspond with the expectations of the data subject.
	What is the impact of the data processing on the data subject and is it beneficial to them
	Are you in a position of power over the data subject and/or are they a vulnerable person?
Cessation of Processing:	In practice can this be stopped at any time at the request of the data subject.

SPECIAL CATEGORIES OF PERSONAL DATA (PREVIOUSLY KNOWN AS SENSITIVE PERSONAL DATA)
This is data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories are set out in the definitions section
In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.
The condition for processing special categories of personal data must comply with the law. If the school does not have a lawful basis for processing special categories of data that processing activity must cease.

STAFF RESPONSIBILITIES
Fully understand your data protection obligations
Check that any data processing activities you are dealing with comply with our policy and are justified by carrying out a data protection impact assessment on each new activity
Do not use data in any unlawful way
Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions.
Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.
DATA PROTECTION IMPACT ASSESSMENT DPIA (for major new projects)
Describe the nature ,scope, context and purposes of processing.
Assess the necessity, proportionality and compliance measures.
Identify and assess risk to individuals and how those risks might be mitigated.

RESPONSIBILITIES OF THE DPO
Keeping the board updated about data protection responsibilities, risks and issues.
Reviewing all data protection procedures and policies on a regular basis.
Arranging data protection training and advice for all staff members and those included in this policy.
Answering questions on data protection from staff, board members and other stakeholders.
Responding to individuals such as clients and employees who wish to know which data is being held on them by us.
Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.
RESPONSIBILITIES OF IT DEPARTMENT
Ensure all systems, services, software and equipment meet acceptable security standards.
Regular checks and scans of security hardware and software to ensure functioning properly.
Researching third-party services the company is considering using to store or process data.
RESPONSIBILITIES OF MARKETING, ALUMNI RELATIONS OFFICER
Approving data protection statements attached to emails and other marketing copy.
Addressing data protection queries from clients, target audiences or media outlets.
Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.
Responsibility for reviewing the activities of the department to ensure that they comply with the lawful bases for processing within the school.

ACCURACY AND RELEVANCE	
Data Processing	Personal Data must be: Accurate, adequate, relevant and not excessive, relative to the purpose for which it was obtained. **Data will be not be processed on any other basis.**
	Corrections requested by individuals: If you believe that information is not correct staff should record the fact that the accuracy of the information is disputed and inform the DPO.
STORING DATA SECURELY **All possible technical measures must be put in place to keep data secure**	
Data on Printed Paper	Must be kept in a secure place with no unauthorised access it. Must be shredded in accordance with the retention policy (see below).
Electronic data stored on computers	Computers and data should be protected with strong passwords which are regularly changed. All computers should be backed up regularly [Refer IT policy].
Data stored in cloud	Refer to IT Policy.
Servers	Must be kept in accordance with the IT Policy (kept in a secure location) and those storing sensitive data adequately protected.
Data stored on CDS Memory sticks	Should be encrypted or password protected and stored locked away as for printed paper and in accordance with the [IT Policy]
Mobile devices/ Personal/school	Data should never be saved directly to mobile devices such as laptops, tablets or smartphones. Always use the school email when transacting school business
DATA RETENTION	
All destruction of data must be in accordance with the school's data protection policy.	
INTERNATIONAL DATA TRANSFER	
There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.	

RIGHTS OF INDIVIDUALS IN RESPECT OF THEIR DATA	
To be informed	A privacy notice is on the school website. The school must keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.
Access:	Individuals may access their personal data and supplementary information by submitting a Subject Access Request and requesting details from the school as set out in the Privacy Policy.
Subject Access Request	An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information.
Rectification	If an individual requests amendments to data which is inaccurate or incomplete this should be carried out without delay within one month extended to two months with the consent of the DPO.
Erasure	If an individual requests that their data is removed and there is no compelling reason for its continued processing it should be deleted.
Restriction of processing	We must comply with any request to restrict, block, or otherwise suppress the processing of personal data. The school is permitted to store personal data if it has been restricted, but not process it further. Enough data should be retained to ensure the right to restriction is respected in the future.
Data Portability	The school is required to provide individuals with their data so that they can reuse it for their own purposes or across different services. This should be provided in a commonly used, machine-readable format, and send it directly to another controller if requested.
To Object	If an individual objects to their data being used the school in accordance with the Privacy Policy the school must cease processing. If there are legitimate grounds for processing which override the interests, right and freedoms of the individual or it relates to to a legal claim then this right will not apply.
Automated decision making	We must respect the rights of individuals in relation to automated decision making and profiling. Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

PROCESS FOR DEALING WITH SUBJECT ACCESS REQUESTS 'SAR's	
To be read in conjunction with the Privacy Policy	
On receipt of an SAR staff should immediately contact their line manager or DPO	
Request by a data subject to see their data which they believe is held by The Hall	**A verbal request is not valid (except if the individual is unable to write)** To be valid the request must be in writing eg. Email, fax, social media. and made to any person in the organisation. Explain that the request must be made in writing, if necessary A third party eg. solicitor may make the request.
The SAR is concerning a child's data	The repose should be made to the child if the school considers that they are mature enough to understand the reasons and implications of the SAR (refer to DPO)
Asking for clarification on SAR	The school is entitled to ask for further information which would help with their response eg. dates of emails
Amendment of requested data	The data supplied must not be amended once a request has been made unless the amendment was pre planned**. To alter the data is a criminal offence.**
Presentation of data	The data must be a capable to being understood by the average individual.
Charge	The maximum discretionary fee for responding to an SAR is £10
Time limit	28 calendar days (regardless of whether a 3dr party is the processor) If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. Approval must be sought from the DPO before extending the deadline
Repeated requests	Please refer to the DPO

DATA PORTABILITY
Any data requested must be provided in a structured, commonly used and machine-readable format .eg CSV file excel or word.

THE INDIVIDUAL'S RIGHT TO ERASURE (THE RIGHT TO BE FORGOTTEN) **A request may be verbal or in writing**	
On receipt of an erasure request staff should immediately contact the DPO	
Individuals have a right to have their data erased and for processing to cease in the following circumstances:	Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed.
	To comply with a legal obligation
	Where consent is withdrawn
	Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing.
	The personal data was unlawfully processed or otherwise breached data protection laws.
	The processing relates to a child
Data cannot be erased in the following circumstances	To exercise the right of freedom of expression and information.
	To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
	For public health purposes in the public interest.
	For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
	The exercise or defence of legal claims
Data relating to a child (under 13)	Parental consent required.
Time limit	One calendar month. (Check the ICO website for the detail)
Fee	No charge unless the request is excessively onerous.
PROCESS TO FACILITATE ERASURE	
Assess whether the data may lawfully be erased	
Collate the data to be erased and ensure that it has not been shared with third parties	
If the data has been shared then the third parties must be contacted and informed of their obligation to erase the data. (If the individual enquires about third parties they must be informed of the sharing of their data)	
Contact the DPO to confirm that the correct procedures have been followed, that the data may be erased.	
Destroy the data using a secure method.	

THE RIGHT TO OBJECT	
The School must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. The School must also offer a way for individuals to object online.	
THE RIGHT TO RESTRICT AUTOMATED PROFILING OR DECISION MAKING	
The school may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:	It is necessary for the entry into or performance of a contract
	Based on the individual's explicit consent
	Otherwise authorised by law.
PROCEDURES	
The school should give individuals detailed information about the automated processing; Offer simple ways for them to request human intervention or challenge any decision about them; and, carry out regular checks and user testing to ensure our systems are working as intended	
THIRD PARTIES	
As a data controller, we must have written contracts in place with any third party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities. The school must only appoint processors who can provide sufficient guarantees under GDPR that the rights of data subjects will be respected and protected.	
CONTRACTS WITH THIRD PARTIES **No member of staff should commit the school to a contract with a third party without contacting the DPO.**	
Most third party providers will have update their terms and conditions to comply with GDPR but it is important to check for this documentation. The minimum conditions for a contract must be:	
Those involved in processing the data are subject to a duty of confidence	The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing
Appropriate measures will be taken to ensure the security of the processing	
The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR;	Notification of data breaches and implementation of Data Protection Impact Assessments; Delete or return all personal data at the end of the contract;
Sub-processors will only be engaged with the prior consent of the controller and under a written contract;	Provide whatever information necessary for the controller and processor to meet their legal obligations; and, nothing will be done by either the controller or processor to infringe on GDPR.

CRIMINAL OFFENCE DATA DBS CHECKS	
The GDPR Rules for special category data do not apply to information about criminal allegations	
To process personal data about criminal convictions or offences	There must be a lawful basis and either a legal or, official authority for processing it.
At The Hall this would apply to the DBS checks carried out as part of safer recruitment. The data is processed in an official capacity but there is no lawful basis to retain a register of criminal offences. The school uses a third party to process data to identify staff with criminal records to which the usual third party rules apply.	
HR are the only department permitted to carry out DBS checks on staff	

AUDIT
A data register is held within the school which contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.
Regular data audits to manage and mitigate risks will inform the data register. A regular data audit will be carried out as defined by the DPO and normal procedures.
TRAINING
Regular GDPR training forms part of staff inset days.
You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities
MONITORING
All staff must observe this policy. The DPO has overall responsibility for this policy. The Hall will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

REPORTING BREACHES
Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach The Hall has a legal obligation to report that data breach to the ICO within 72 hours including weekends and bank holidays.
Examples are the loss of a USB stick; data being destroyed or sent to the wrong address; the theft of a laptop; or, hacking.
All members of staff have an obligation to report actual or potential data protection compliance failures in order to investigate the failures and take remedial steps if necessary and the DPO should maintain a register of compliance failures
Staff should contact the DPO and notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures.
Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action. Please refer to the whistleblowing policy for our reporting procedures.

PROCEDURE FOR REPORTING A BREACH	
Call the ICO : 0303 123 1113	
Be prepared to disclose	What has happened.
	When and how you discovered the breach.
	The people who have or may be affected by the breach.
	What you are doing as a result of the breach.
	Who the ICO should contact for more information.
	Who else you have told.

FAILURE TO COMPLY
The school takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.
The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under school procedures, which may result in dismissal
If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

END OF POLICY