KINGHAM HILL SCHOOL

Data Protection Policy

1. Introduction

- **Scope.** Kingham Hill School is required to put in place proportionate organisational and technical measures to manage the risks associated with the personal data staff process. The School also needs to protect sensitive operational and commercial business information. The School is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with data protection legislation. The School processes personal data about our staff, pupils, suppliers and other individuals for a variety of business purposes. This policy sets out how the School seeks to protect personal data and ensure that our staff understand the rules governing the use of the personal data to which they have access during their work. This policy requires staff to ensure that the Data Compliance Officer be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

- **Interpretation.** The 'Data subject' means an individual who is the subject of personal data. The 'Data Controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed. A 'Third Party', in relation to personal data, relates to any person other than the data subject, the Data Controller, or any other person authorised to process data for the Data Controller. 'Staff' refers to all individuals 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. Subheadings are for ease of reading and do not form part of the policy.

- This policy does not form part of a contract of employment and may be amended by the School at any time.

2. Application

- Kingham Hill School is required to evidence how the organisational and technical measures it puts into place support the development of a culture of data protection. Furthermore, the School is required to evidence where its policies, processes and procedures have not been followed and take action against individuals who do not comply so that their behaviour is dissuasive to others.

- The School has a legal duty to ensure that all personal and sensitive information we process is managed in line with the principles set out in data protection law and are regulated by the Independent Schools Inspectorate.

- The School will comply with the principles of the European Union General Data Protection Regulation (GDPR) 2016, the Data Protection Act (DPA) 2018 and any other associated applicable data protection legislation.

- This policy applies to all staff who handle personal and/or special category data or information on behalf of Kingham Hill School whether this is paper-based, electronic or in any other formats including spoken information.

- Staff are personally responsible at all times for the personal and/or special category data, in whatever format, in their care. They must safeguard the security of personal and/or special category for which they are responsible or which they access, to carry out their work.

- The School will enforce this policy through its procedures and policies. Breaches of this policy could lead to disciplinary action and penalties up to and including dismissal, depending on the breach and its impact on the School and data subject(s).

3. Data Protection Principles

- The General Data Protection Regulations are formulate around a set of key principles, namely:

    - 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
    - Limited for its purpose: Data can only be collected for a specific purpose
    - Data minimisation: Any data collected must be necessary and not excessive for its purpose
    - Accurate: The data we hold must be accurate and kept up to date
    - Retention: We cannot store data longer than necessary
    - Integrity and confidentiality: The data we hold must be kept safe and secure.

- The School use personal data for personnel, administrative, financial, regulatory, payroll, teaching and learning and business development purposes. Business related activities include the following:

    - Compliance with our legal, regulatory and governance obligations and good practice
    - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
    - Ensuring policies are adhered to (such as policies covering email and internet use)
    - Administrative purpose e.g. admission, HR, alumni, safeguarding (pastoral), recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting
    - Investigating complaints
    - Checking references, ensuring safe working practices, monitoring and managing student and staff access to systems and facilities and student and staff absences, administration and assessments
    - Monitoring staff conduct, disciplinary matters
    - Marketing ourselves

- Improving services.

4. Data Controller

- The Kingham Hill Trust is classified as the Data Controller. The Trust must maintain its appropriate registration with the relevant supervisory authority e.g. Information Commissioner's Office (ICO) in the UK to continue lawfully processing data.

- The Data Controller in the guise of the Kingham Hill School Trust Secretary is responsible for monitoring compliance with data protection and associated law. The Data Controller delegates local responsibility for this task to the School's Data Compliance Officer, who is the Bursar (dco@kinghamhill.org).

- The ICO registration number for the Kingham Hill Trust is Z5641099.

5. Definitions

- 'Personal data' refers to 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. The personal data gathered may include but is not limited to: individuals' phone number, email address, IP address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, family make-up, dependants, next of kin, health information and images.

- '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.

- '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
    - Restriction
    - Erasure or destruction.

6. Accountability and transparency

- The School must ensure accountability and transparency in all its use of personal and sensitive data. To do this it must evidence that it complies with each of the six Principles. It does this by:

    - Implementing all appropriate technical and organisational measures
    - Maintaining up to date and relevant documentation on all processing activities
    - Conducting Data Privacy Impact Assessments (where necessary)
    - Implementing measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation/anonymisation
    - Transparency
    - Informing individuals of the processing of their information.

7. Processing requirements

- The School must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that it should not process personal data unless the individual whose details it is processing has consented to this happening or a condition for processing has been identified.

- If the School cannot apply a lawful basis (explained below), its processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

- The data protection legislation provides that the responsibilities of a Data Controller is to:

    - Analyse and document the type of personal data we hold
    - Ensure compliance with the rights of the individual
    - Identify the lawful basis for processing data
    - Ensuring consent procedures are lawful
    - Implementing and reviewing procedures to detect, report and investigate personal data breaches
    - Store data in safe and secure ways
    - Assess the risk that could be posed to individual rights and freedoms should data be compromised.

- All staff must ensure that they:

    - Fully understand their data protection obligations
    - Any new processing activity they are dealing with complies with the School policies and is justified
    - Do not use data in any unlawful way
    - Do not store data incorrectly, be careless with it or otherwise cause the School to breach data protection laws and our policies through their actions
    - Comply with this policy at all times

- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations to the Data Compliance Officer (DCO) without delay.

8. Lawful basis for processing data

- The School must establish a lawful basis for processing data, ensuring that any data it is responsible for managing has a recorded lawful purpose. At least one of the following conditions must apply whenever the School process personal data:

  - **Consent.** Where necessary the School hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose
  - **Contract.** The processing is necessary to fulfil or prepare a contract for the individual
  - **Legal obligation.** The School has a legal obligation to process the data (excluding a contract)
  - **Vital interests.** Processing the data is necessary to protect a person's life or in a medical situation
  - **Public function.** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law
  - **Legitimate interest.** The processing is necessary to the School's 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.

9. Deciding which processing condition to rely on

- The School's commitment to the first Principle requires it to document this process and show that it has considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

- It must also ensure that individuals whose data is processed by the School are informed of the lawful basis for processing their data, as well as the intended purpose. This is done via a privacy notice. This applies whether the School has collected the data directly from the individual, or from another source. Privacy notices are linked to the information populated in data mapping. The School's privacy notices are available via the School website at https://www.kinghamhill.org.uk/about/policies or by contacting Reception.

10. Special categories of personal data

- Previously known as sensitive personal data, this relates to data about an individual which is deemed to be 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.

- In most cases where the School processes special categories of personal data it requires the data subject's explicit consent to do this unless exceptional circumstances apply, or the School is required to do this by law (e.g. to comply with legal obligations to ensure safeguarding). 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 then processing activity must cease.

- Additionally to establishing a lawful basis for processing personal information the School must also establish a lawful basis for processing special category data. At least one of the following conditions must apply whenever we process special category data (Article 9):

    - Consent
    - Employment law
    - Vital interests
    - Legitimate activities
    - Made public by data subject
    - Establishment, exercise or defence of legal claims
    - Public interest on the basis of Union or Member State law
    - Health or social care
    - Public interest in the area of public health
    - Public interest in the area of archiving, scientific or historical research or statistical purposes.

11. Responsibilities of the Data Compliance Officer (DCO)

- The DCO is responsible to the Data Controller for:

    - Keeping the Board of Governors 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
    - Answer questions on data protection from staff, governors and other stakeholders
    - Responding to individuals (data subject) who wish to know which data is being held on them by Kingham Hill School
    - Ensuring that third parties that handle the company's data have a contracts or agreement in place regarding data processing and the data controller/data processor responsibilities.

- The DCO is supported in their role by the SMT and HR Support Officer and IT Manager, who are trained in Data Protection and act as alternative points of contact in the absence of the DCO.

12. ICT support

- The IT Manager is responsible to the DCO for:

    - Ensuring all systems, services, software and equipment meet acceptable security standards
    - Checking and scanning security hardware and software regularly to ensure it is functioning properly

- Researching third-party services, such as cloud services the School is considering using to store or process data.

13. Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be in line with the School IT policies.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- Any cloud-based system used to store data needs to be registered on the Kingham Hill School mapping toolkit.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the School backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones unless the appropriate technical and organisational measures are in place.
- All servers containing special category data must be approved and protected by security software.
- All possible technical measures must be put in place to keep data secure.

14. Data retention

- We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained. These are reflected in the Data Tracking and Retention of Information Policy.

15. Transferring data internationally

- There are restrictions on international transfers of personal data. Staff must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without having this registered onto the data map and making the Data Compliance Officer or IT Manager aware.

16. Rights of individuals

- Individuals have rights to their data which the School must respect and comply with to the best of its ability (also see Information Rights Policy). We must ensure individuals can exercise their rights in the following ways:

    - **Right to be informed.** Articles 13 and 14 of the GDPR specify what individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

    - **Right of access/Subject Access Request.** The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why the School is using their data, and check it is doing it lawfully.

- **Right to rectification.** Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified.

  An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

- **Right to erasure and how to comply.** Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

- **Right to data portability.** The right to data portability gives individuals the right to receive personal data they have provided to a Data Controller in a structured, commonly used and machine readable format. It also gives them the right to request that a Controller transmits this data directly to another Controller.

- **Right to object.** Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask the School to stop processing their personal data. The right to object only applies in certain circumstances. Whether it applies depends on the purposes and lawful basis for processing.

- **Right in relation to and right to restrict automated profiling or decision making.** The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

- In the absence of the DCO, the SMT and HR Support Officer or IT Manager should be contacted with any immediate queries. During the absence of the DCO, all emails sent to the DCO@kinghamhill.org will be automatically forwarded to 9ine Consulting who will ensure that data subject queries are considered and responded to. 9ine Consulting are a data processor processing under clear contractual arrangements.

17. Privacy notices

- A privacy notice must be supplied at the time that data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month. The School Privacy Notices for Parent and Pupils are provided to families upon offer of a place. The School Privacy Notice for Staff is shared with them upon the initiation of their contract.

- If disclosure to another recipient is envisaged, then the privacy notice for the third party must be supplied prior to the data being disclosed.

18. Using third party controllers and processors

- As a data processor on behalf of the Kingham Hill Trust, the School must have written contracts in place with any third-party data controllers and/or data processors that we share information with and or process information for. 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 data protection legislation.

- As a data processor on behalf of the Kingham Hill Trust, the School must only act on the documented instructions of the Controller. The School acknowledges its responsibilities as a data processor under data protection legislation and it will protect and respect the rights of data subjects.

19. Contracts

- The School's contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. The School's contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller. These will be specified in the data processing agreements and may be further supported by a data sharing agreement and/or a privacy impact assessment.

- At a minimum, the School's contracts must include terms that specify:

    - A processor can act only on written instructions
    - Those involved in processing the data are subject to a duty of confidence
    - Appropriate measures will be taken to ensure the security of the processing
    - Sub-processors will only be engaged with the prior consent of the controller and under a written contract
    - The School will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
    - The processor will assist the School in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
    - A processor will delete or return all personal data at the end of the contract
    - A processor will submit to regular audits and inspections and provide whatever information necessary for the insert name and processor to meet their legal obligations
    - Nothing will be done by either the School or processor to infringe on GDPR.

20. Criminal offence data/Criminal record checks

- The Data Protection Act 2018 which supplements the GDPR authorises the use of criminal records checks by organisations other than those vested with official authority i.e. the ICO. The Act allows Kingham Hill School to process criminal convictions data where necessary for the purposes of performing or exercising employment law obligations or rights. The School carry out such processing, in accordance with the principles of the Act and the School's erasure and retention policies.

- The Act also authorises processing criminal records data in other circumstances, including where the subject has given his or her consent. This would allow the School to request a criminal records check where the prospective employee agrees to this, provided that the consent meets the specific requirements under the GDPR.

- All data relating to criminal offences is a special category of personal data and must be treated as such.

21. Audits, monitoring and training/Data audits

- Regular data audits to manage and mitigate risks will inform the School's data mapping toolkit. This is to contain 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.

22. Reporting breaches

- Any breach of this policy or of data protection laws must be immediately reported to the DCO. As soon as a staff member becomes aware of a breach, the School has a legal obligation to report any high risk data breaches to the supervisory authority within 72 hours. For full details see the Data Breach Policy.

- All members of staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows the School to:

    - Investigate the failure and take remedial steps if necessary
    - Maintain a register of compliance failures
    - Notify the ICO of any compliance failures.

- Any member of staff who fails to notify of a breach/incident 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. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under the School's procedures which may result in dismissal.

23. Policy Links

- Privacy Notice for Staff
- Privacy Notice for Pupils, Parents and Visitors
- IT Acceptable Use Policy for Staff
- IT Acceptable Use Policy for Pupils, Parents and Visitors
- Parental Contract
- Data Tracking and Retention of Information Policy
- Information Handling Guidance

This policy was ratified on …….

and will be reviewed May 2020

Signed by the Chairman of Governors ……

Reviewed and updated by Catriona Thompson (May 2019)