LAMBROOK

NURTURING
POTENTIAL
SINCE 1860

Data Protection Policy

This document applies to all parts of Lambrook School including the Early Years Foundation Stage.

Reviewed February 2025 Review Date: February 2026

Lambrook School – Our Purpose

Since 1860, Lambrook has been laying the foundations for its pupils' futures. Children have one opportunity for an education which will form the basis of their lives and, at the same time, one childhood; Lambrook aims to keep a happy balance between the two.

During their time with us, we give our pupils the 'Feathers to Fly' so that when they leave us, they will spread their wings and will take flight; leaving Lambrook as confident, happy, engaging, independent and kind young people who are outward looking in all that they do.

Inspiring

Inspiring pupils from Nursery through to Year 8, offering the most outstanding breadth of educational experiences, encouraging academic intrigue and a desire to learn.

Nurturing

Nurturing and supporting all pupils through an outstanding level of pastoral care, empowering pupils to flourish and have healthy relationships with others within our vibrant and caring School community.

Providing

Providing pupils with an abundance of opportunities to discover, pursue and develop their skills, talents and interests.

Preparing

Preparing our children for the next stage of their educational journey, developing the many 'feathers' necessary for their time at Lambrook, at their future senior schools and beyond.

Equipping

Equipping our children with the skills and the confidence to understand the challenges of the world in which they live; recognising their responsibility towards others, the environment and themselves and enabling them to make a difference, both now and in the future.

The School is registered under the Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR).

About this Policy

Everyone has rights with regard to the way in which their personal data is handled. During the course of the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful School operations.

This policy bears relation to other policies existing in school:

- Privacy Note for Parents and Pupils
- Privacy Note for Staff
- Records and Retention Policy
- Induction, Training and Development of Staff Policy
- Staff Code of Conduct
- Whistleblowing Policy

Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Any breach of this policy may constitute a breach of the Staff Code of Conduct and an allegation of misconduct.

This policy sets out the basis on which the School will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

General Statement of the School's duties

The School is required to process relevant personal data regarding its data subjects (staff, pupils, their parents, suppliers and other third parties) as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Note: data includes all information held by the school whether in electronic format or a paper based storage system.

Data Controller

While the School is the Data Controller, the School has appointed Lesley Hailey, the Compliance Officer, to act on behalf of the School as Data Privacy Officer (DPO) . Lesley Hailey (DPO) will endeavour to ensure that all personal data is processed in compliance with the General Data Protection Regulation (2018). Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Controller.

The Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the Data Protection Act 1998. These provide that personal data must be: -

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive

- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Personal Data

Personal data covers information relating to identifiable individuals, such as pupils, job applicants, current and former employees, agency, contract and other staff, pupils and their parents, suppliers and marketing and business contacts. It includes expressions of opinion about the individual, any indication of someone else's intentions towards the individual, information necessary for employment such as the worker's name and address and details for payment of salary.

Processing of Personal Data

The School's policy is to process personal data in accordance with the applicable data protection laws as set out above. All staff have a personal responsibility for the practical application of this policy.

Staff should generally not process personal data unless:

- The individual whose details are being processed has consented to this;
- The processing is necessary to perform the Schools legal obligations or exercise legal rights, or
- The processing is otherwise in the School's legitimate interests and does not unduly prejudice the individual's privacy.

Staff need to be aware of the importance of the instances in which they are processing personal and sensitive data about their employees. These may include:

- Telephone conversations
- Emails
- Notifications
- Meetings
- Meeting agendas and minutes
- Class lists
- Team sheets
- Exercise books
- Art work
- Scrap books
- Display work
- Seating plans

Much of this processing will take place as part of a Staff member's everyday duties and to ensure the successful functioning of the School in ensuring its aims. However, the access to that data of people who may **not** be entitled to process that information must be considered:

- Visitors in school viewing a list, display or notice featuring pupils' names and information
- People outside the Lambrook community overhearing a conversation
- Members of the public viewing a device or laptop screen
- Misplaced devices, laptops, potable drives, USB sticks
- Emails featuring private or sensitive data sent in error to the wrong recipient (misspelt or auto-fill)

- Phishing attacks that retrieve usernames and passwords
- Other colleagues not privy to sensitive or highly confidential information accessing information left on a desk or in a meeting about another colleague, parent or pupil
- Email, message or Calendar notifications on unattended devices allowing others to view personal, sensitive or highly confidential appointments or communications

When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used.

There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the DPO.

Sensitive Personal Data
The School may, from time to time, be required to process sensitive personal data regarding an employee. Where sensitive personal data is processed by the School, the explicit consent of the data subject will generally be required in writing.

The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

Processing of Credit Card Data
The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, please seek further guidance from the Director of Finance.

Accuracy, adequacy, relevance and proportionality
Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the School to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the DC.

Staff must ensure that personal data held by the School relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the DC so the School's records can be updated.

Rights of Individuals
Staff members, parents, members of the public and any other data subjects have the right of access to information held by the School, subject to the provisions of the General Data Protection Regulations (2018).

Any employee or indeed any data subject wishing to access their personal data should make a Subject Access Request to the DPO. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to information request. The School may charge £10 for the provision of

the requested personal data, as permitted by law. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the School's attention. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.

Staff should not send direct marketing material to someone electronically (e.g. by email) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the DPO about any such request. Staff should contact the DPO and the Head of External Relations for advice on direct marketing before starting any new direct marketing activity.

Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPO.

Accuracy

The School will endeavour to ensure that all personal data held in relation to workers is accurate and kept up to date. Staff members and, in some cases parents, must notify the HR Manager of any changes to information held about them. The data subject (e.g. staff member) has the right to request that inaccurate information about them is modified or erased.

Timely Processing

The School will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required. For further information on timescales, please see the Record and Retention Policy.

Enforcement

If an employee believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the Staff member should refer this either through the Low-Level Concerns Policy, the Whistleblowing Policy or, if it relates to an incident affecting them personally, the School's Grievance Policy. The employee should also notify the DPO.

If a Staff member is aware that they have breached GDPR by, for example, misplacing a laptop, inadvertently sending data by email to the wrong recipient, being overheard in a conversation they should self-refer using the referral form on SharePoint as soon as practically possible – including full details of the information involved, how it has been processed and other parties involved. Even if the Staff member is unsure whether confidential information has been disclosed or if they feel they may have been targeted as part of a phishing attack, they should act as if there has been a breach and complete the self-referral. The Staff member should also inform the Bursar and Deputy Head and alert them to the potential GDPR breach. The Referral Form will direct the staff member to notify other colleagues, depending on the circumstances e.g. the IT dept, External Relations

The Deputy Head and Compliance manager can then, if appropriate, pass on the breach to the School's DPO, Judicium via the Breach section of the Jedu portal. Breaches - Judicium

Data Security

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to both staff and pupils.

As such, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headmaster or Director of Finance.

Where an employee is permitted to take data offsite, security measures will be observed. These might include: data existing as password protected cloud-based documentation; two-factor authentication; device passcodes and Touch ID.