DATA PROTECTION POLICY

1. OVERVIEW

1.1 Policy Statement

This policy outlines the John Lyon School and Quainton Hall School ("the School") approach to complying with the Data Protection Act 2018 and the EU and UK General Data Protection Regulation (GDPR).

The John Lyon School (No. Z8500124) and Quainton Hall School (No. Z8950892) are registered Data Controllers as part of John Lyon's Foundation. They are committed to complying with all relevant UK & EU laws in respect of personal data and the protection of the 'rights and freedoms' of individuals whose information they collect and process.

1.2 Policy Owner

The Data Protection Policy is owned by the nominated Privacy Officer, the Chief Operating Officer (COO), Gareth Mawdsley (DataProtection@johnlyon.org).

1.3 Policy Audience

All members of staff at School who are involved in the processing, storage, modification or deletion of personal data are obliged to comply with this policy when doing so. The policy may be shared with third parties so that they will understand what they are expected to do to support the School fulfil its data protection obligations.

Any third party working with or on behalf of the School that have, or might have, access to personal data will be expected to have read, understood and to comply with this policy or be committed to an equivalent approach to regulatory compliance.

1.4 Effective Date

This policy is effective from 1 April 2022.

This policy will be reviewed on a regular basis and in any event not later than every 12 months from the effective date.

1.5 Policy Governance

1.5.1 Dispensations

If an area of the school cannot comply with one or more of the requirements set out in this policy, a formal request for a dispensation must be submitted to the Privacy Officer for approval with suggested mitigatory actions. Any dispensations must be agreed between the Privacy Officer and the person responsible for privacy of the affected area.

The Privacy Officer must maintain a register of dispensations and a privacy risk register.

Any dispensations must be reviewed and updated annually.

1.5.2 Policy Non-Compliance

Non-compliance with this policy, where an approved dispensation is not in place, must be reported to the Privacy Officer at DataProtection@johnlyon.org.

Any member of the staff not complying with this policy may be subject to disciplinary action.

1.6 Related Documents

All staff have a responsibility to handle the personal data that they come into contact with fairly, lawfully, responsibly, and securely and in accordance with all relevant School policies and procedures.

In particular, there are data protection implications across a number of areas of the School's wider responsibilities, such as safeguarding and IT security, so all staff should read and comply with the following policies, all of which can be located in the Staff Handbook:

- Safeguarding and Child Protection Policy
- IT Policy for Staff, Pupils, Parents, Governors and Visitors
- Online Safety Policy
- Photographic Images Policy
- Privacy Notice

2. POLICY STATEMENTS

2.1 Data Protection Principles

The GDPR sets out six principles relating to the processing of personal data that must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specific and explicit purposes and used only for the purposes it was collected for;
3. Relevant and limited to what is necessary for the purposes for which it is processed;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary for the purposes for which it is processed; and
6. Processed in a manner that ensures appropriate security of the personal data.

In addition, the GDPR's 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful.

The School must be able to demonstrate compliance with the above points.

Any queries or clarifications on how this is achieved should be directed to the Privacy Officer at DataProtection@johnlyon.org.

2.2 Data Protection Policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (e.g. including parents, current and prospective; pupils, prospective, current and alumni; employees, prospective, current and past).

Key data protection terms used in this data protection policy are:

- **Data controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or personal data)** – any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Special categories of personal data** – as defined by the GDPR these are: data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual.

Please note that the School only controls data about two of these special areas: medical conditions and religious belief, and both are for the legitimate interest of running the School safely and efficiently.

2.3 Privacy Notice

The School has a Privacy Notice that contains specific information that must be provided to the data subject. This, as a minimum, includes:

- the identity and the contact details of the controller and, if any, of the controller's representative.
- the contact details of the Privacy Officer.
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
- the period for which the personal data will be stored.
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected.
- the categories of personal data concerned.
- the recipients or categories of recipients of the personal data, where applicable.
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data.
- any further information necessary to guarantee fair processing.

3. RESPONSIBILITIES

The School acts as a data controller when managing personal data that relates to pupils, parents, internal operations, staff members, prospects and job applicants.

The Privacy Officer is responsible for overseeing compliance with GDPR and other relevant laws across the School.

Senior management and all those in managerial or supervisory roles throughout the School will be responsible for developing and encouraging good information handling practices.

3.1 Data Protection Officer

The School has appointed a Data Protection Officer, Privacy Culture who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the GDPR. 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 Privacy Officer contactable via DataProtection@johnlyon.org

3.2 Data Champion

A responsible person will be nominated as the Data Champion for each School Department where personal data is processed.

The Data Champion will be responsible for ensuring this policy is followed in their area of responsibility and they will be assisted by other staff members who will support them from an operational perspective.

It is the responsibility of the Data Champion to:

- Engage with the Privacy Officer in a proactive manner.
- Maintain a set of personal data flows for their area of responsibility.
- Ensure that staff in their area of responsibility are adequately trained and informed of their data protection responsibilities.
- Ensure the Privacy Officer is made aware of any personal data incidents or breaches.
- Prepare a monthly report that summarises activity in their area of responsibility.
- Populate GDPR registers as required.

Data Champions will be supported by the School Privacy Officer.

4. MANAGING GENERAL DATA

4.1 General

It is the responsibility of all staff members of the School to ensure that the departments in which they operate work to this policy and related documents, can evidence compliance and ensure that they are fully aware of their roles and responsibilities.

4.2 Employee Data

4.2.1 Basis for Processing

Personal data on staff members is processed under their contract of employment.

Job applicants provide their data with a view to entering into a contract if their application is successful. The basis for processing their data is also contract.

4.2.2 Principles for Processing

- All employees will work proactively with the School to ensure their personal data is maintained accurately.
- Employee data will not be shared unless specifically stated in the contract.
- All employees have the right to raise a data subject request.
- Any employee who is dissatisfied with the way their personal data has been handled by the School may raise a complaint via DataProtection@johnlyon.org.
- All employees have the right to lodge a complaint with their local data protection Authority – the ICO in the UK.

4.3 Parents and Pupils Data

4.3.1 Basis for Processing

Personal data processed on behalf of a parent will be conducted under contract, legitimate interest and/or to comply with legal requirements.

Personal data processed on behalf of pupils will be conducted under:

- Legitimate interest.
- Legal obligation
- Consent.
- Contract.

All processing conducted on behalf of the above will be in line with this policy and in accordance with all applicable laws.

4.3.2 Principles for Processing

The School will process parents and pupils' data in compliance with the Data Protection Principles as stated in section 2.1 of this Policy.

4.4 John Lyon Foundation

As part of our commitments across the wider John Lyon Foundation, the School might share personal data with:

- The **John Lyon Foundation** (comprising the **John Lyon Corporation** and the **John Lyon Charity** (registered charity number 237725))
- The **John Lyon Corporation** (The Keepers and Governors of the Possessions, Revenues and Goods of the Free Grammar School of John Lyon, within the town of Harrow-on-the-Hill (registered charity number 310033), comprising **Harrow School** and **John Lyon School**, and with subsidiaries the **Harrow International Schools Limited** (HISL) and **Harrow School Enterprises Limited** (HSEL))
- **Harrow School** where administrative functions are shared with the John Lyon School.

All processing conducted on behalf of the above will be in line with this policy and in accordance with all applicable laws.

5. DATA SUBJECT RIGHTS

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated processing.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used, and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

The School will ensure that data subjects may exercise these rights.

Procedures to support the enforcement of these rights can be found within the School's Privacy Framework. These procedures describe how the School will ensure that its response to the data subject request complies with the requirements of GDPR

5.1 Complaint Handling

Data subjects have the right to complain to the School in relation to the processing of their personal data, the handling of a request or how complaints have been handled in line with the complaints procedure.

Any comments or queries on this policy should be directed to DataProtection@johnlyon.org.

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with data protection law, they should utilise the School's Complaints Procedure for Parents and should also notify the Head (Head@johnlyon.org).

You can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator. Information for the public is available from the ICO.

6. PERSONAL DATA SECURITY

All Staff members are responsible for ensuring that any personal data that the School holds and for which they are responsible, is kept securely. All personal data will be held in accordance with the IT Policy.

Personal data will not be disclosed to a third party unless that third party has been specifically authorised to receive the information and has entered into a signed agreement with the School that incorporates both confidentiality and the approval to process such data.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with their role in the business. All personal data should be treated securely and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with the information security policy; and/or
- stored on (removable) computer media which are encrypted, in line with the information security policy.

Manual records that include personal data should only be removed from business premises if strictly necessary to do so.

More generally, we require all School staff to remain conscious of the data protection principles to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information.

All members of staff with management responsibilities must be particular champions of these principles and oversee the swift reporting of any concerns about how personal information is used by the School to the Privacy Officer and identify the need for (and implement) regular staff training.

6.1 Security Measures

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. Online and digital security is maintained by staff following the appropriate sections of the IT Policy.

6.2 Personal Data Incidents & Breach

One of the key new obligations contained in the GDPR concerns reporting personal data breaches. Data controllers must report certain types of personal data breach (those that risk an impact to individuals) to the ICO within 72 hours of the initial discovery.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must notify the School's Privacy Officer. If staff are in any doubt as to whether or not you should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about it to make a decision.

6.3 Data Protection Impact Assessment

A data protection impact assessment (DPIA) will be conducted whenever a new service involving personal data is being developed.

The DPIA will be sub-divided into two elements; (1) screening, and (2) full DPIA.

It will be the responsibility of all activity owners to complete a screening questionnaire as outlined in the DPIA procedure. A copy of the completed screening questionnaire will be stored along with project documentation and be available for audit purposes. The screening questionnaire, which will be conducted for every activity, will be used to identify whether a full DPIA is required or not.

Before a full DPIA is undertaken the Privacy Officer will be consulted to determine if one is required or not. The procedure for conducting a DPIA can be found in the School's Privacy Framework.

7. THIRD PARTIES

Any third-party business service providers working with or for the School that have, or might have, access to personal data will be expected to have read, understood and to comply with this policy.

All third-party processors must commit to complying with GDPR.

All third-party processors must have a contract in place, with suitable data protection clauses, before the processing of personal data commences.

No third party may access personal data held by the School without first having entered a contract or in the absence of a contract, a data processing agreement. This will impose obligations no less onerous than those which the School is committed to on the third party.

Any sub-processors appointed by the third party must be approved, in writing, by the School.

8. RETENTION AND DISPOSAL OF DATA

Personal data may only be deleted or disposed of in line with the archiving procedures of the School, laid down in the Data Asset Register.

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School at DataProtection@johnlyon.org if you believe that your personal data is inaccurate or untrue or if you are dissatisfied with the information in any way.

Similarly, it is vital that the way you record the personal data of others – in particular colleagues, pupils, and their parents – is accurate, professional and appropriate.

9. DATA TRANSFERS

All exports of data from within the European Economic Area (EEA) to third countries, outside the EEA, must have an adequate level of protection in place.

Whenever a third-party processor intends to or is processing data in a third country, the Privacy Officer must be informed without delay.

10. DISCLOSURE OF DATA

The School must ensure that personal data is not disclosed to unauthorised third parties. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to consider whether or not disclosure of the information is relevant to, and necessary for, the conduct of the School's activities.

Any requests to share personal data with third parties, out of the course of normal business operations, should be referred to the Privacy Officer and must be supported by appropriate documentation.