



EMPLOYEE PRIVACY NOTICE

1. OVERVIEW

This Privacy Notice will help you understand how and why we collect personal data about you and what we do with that information. It also explains the decisions you can make about your own information. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** (the 'GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this privacy notice.

2. WHO WE ARE?

The John Lyon School [no. Z8500124] (incorporating both John Lyon Senior and Quinton Hall Prep) is a registered Data Controller as part of the John Lyon's Foundation. We are committed to complying with all relevant UK and EU laws in respect of personal data and the protection of the 'rights and freedoms' of individuals whose information they collect and process.

The School will follow procedures that aim to ensure that all employees, workers, volunteers and consultants who have access to any personal data held by or on behalf of the School are fully aware and abide by their duties and responsibilities under current data protection legislation, the School's Data Protection Policy and other School policies, procedures and guidance. In this context, consultants are self-employed individuals who work as part of the School's staff.

3. RESPONSIBILITY FOR DATA PROTECTION

The School is a **Data Controller** and is responsible for determining how personal data is processed and for what purpose.

The School has a Privacy Officer, the Chief Operating Officer (COO), Gareth Mawdsley who is responsible for managing how we look after personal data and deciding how it is shared. He can be contacted at DataProtection@johnlyon.org.

The Privacy Officer will respond to all your requests and enquiries concerning the School's uses of your personal data and will ensure that all personal data is processed in compliance with this privacy notice, the School's Data Protection Policy, and other School policies, procedures and guidance and data protection legislation.

4. WHAT THIS PRIVACY NOTICE IS FOR

This privacy notice is intended to provide information about how the School will use (or 'process') personal data about individuals. It applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this privacy notice. You should read this privacy notice alongside your contract of

employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

We will hold data in accordance with our Data Retention and Disposal Procedure and Data Retention Schedule. A copy of this can be obtained from the School's Privacy Officer. We will only hold data for as long as necessary for the purposes for which we collected it.

This privacy notice does not form part of your contract of employment (or contract for services if relevant) and can be amended by the School at any time. It is intended that this privacy notice is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this privacy notice, the School intends to comply with the 2018 Act and the GDPR.

5. HOW WE DEFINE PERSONAL DATA

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It does not include anonymised data.

This privacy notice applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor or the HMRC). It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any aptitude tests and pre-employment assessments including a health assessment questionnaire or an occupational health assessment;
- reference details provided by your former employers or alternative referees;
- your contact details, home address and date of birth;
- the contact details for your emergency contacts, including your marital status and family details;
- your gender and other equalities data (e.g.: race, nationality, age, disability status);
- information about your contract of employment (or for services) including start and end dates of employment/engagement, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and other financial information, e.g. student loans, attachment of earnings orders and information in relation to your tax status including your national insurance number;
- your identification documents including passport, birth certificate and driving licence, copies of utility bills and bank statements and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;

- electronic information in relation to your use of IT systems/swipe cards/telephone systems/entry systems;
- your images (whether captured on CCTV, by photograph or video);
- car details (about those who use our parking facilities); and
- any other category of personal data which we may notify you of from time to time.

6. HOW WE DEFINE SPECIAL CATEGORIES OF PERSONAL DATA

The School may need to process special category personal data (concerning health, ethnicity, religious or philosophical beliefs, genetic or biometric data, sexual orientation) or criminal records information such as criminal convictions and offences in accordance with rights and duties imposed on it by law, including safeguarding and employment legislation, or from time to time by explicit consent where required. The reasons for processing special category data may include:

- Statutory pre-employment checks such as DBS checks, Overseas Police Checks and Barred List checks to safeguard pupils' welfare.
- Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duty of care.
- To run any of its systems that operate on biometric data, such as for security, health & safety and other forms of staff identification.

We may hold and use any of these special categories of your personal data in accordance with the law.

7. HOW WE DEFINE PROCESSING

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

8. HOW WILL WE PROCESS YOUR PERSONAL DATA?

The School will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal, statutory and safeguarding obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You

have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in the section below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details, we would not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

9. EXAMPLES OF WHEN WE MIGHT PROCESS YOUR PERSONAL DATA

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example (and see the section below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract or agreement with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities and employee wellbeing*;
- to monitor and protect the security (including network security) of the School, of you, our other staff, pupils and others;
- to monitor and protect the health and safety of you, our other staff, pupils, visitors and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- to pay tax and national insurance;
- to provide a reference upon request from another employer;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, safeguarding legislation, tax law and other laws which affect us*;
- to comply with ISI, ISC and DfE requirements (census data etc);
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- the prevention and detection of fraud or other criminal offences;

- to defend the School in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- for any other reason which we may notify you of from time to time.

We do not need your consent to process special category data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- for legal and regulatory purposes such as child protection and safeguarding, this includes DBS checks and Barred List checks as well as Overseas Police Checks;
- for diversity monitoring and health and safety;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational health or for the assessment of your working capacity.

* We might process **special categories of your personal data** for the purposes set out in the paragraphs above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, nationality, religion or gender to monitor equal opportunities and comply with our obligations under gender pay reporting;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety;
- to run any systems that operate on biometric data, such as for security and other forms of employee identification.

10. HOW THE SCHOOL COLLECTS DATA

Generally, the School receives personal data from the individual directly. This may be via a form or simply in the ordinary course of interaction or communication (such as e-mail or written communication).

In some cases, personal data may be supplied by third parties (for example other professionals or authorities working with that individual).

11. WHO HAS ACCESS TO YOUR PERSONAL DATA AND WHO WE SHARE IT WITH?

Sometimes we might share your personal data with third parties such as professional advisers (lawyers, accountants, insurance companies etc) or relevant authorities (for example, HMRC, Home Office, pension providers, police, safeguarding agencies) to carry out our obligations under our contract with you or for our legitimate interests. A full list of 3rd parties can be found in the school's Processor Register.

Examples of such legitimate activities would be the sharing of relevant data with the organisation that processes the School's DBS applications; the School's Occupational Health Advisers (with your consent), and the Independent School's Council for their annual census.

The School is under duties imposed by law and statutory guidance (including *Keeping Children Safe in Education*) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on HR or safeguarding files, and in some cases referrals to relevant authorities such as the LADO (Local Authority Designated Officer). For further information about this please view the School's Safeguarding Policy.

In accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

We require those individuals or organisations to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We may share personal data with employee's line managers for the purposes of day to day people management activities (such as absence management, where we might share an occupational health report with your manager) and management planning. Line Managers are required to keep your personal data confidential and secure and to protect it in accordance with the law and our policies.

We do not normally send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

12. HOW LONG WE KEEP PERSONAL DATA

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary employee files is up to seven years following departure from the School. However, health and safety incident reports and information related to safeguarding will need to be kept much longer in accordance with specific legal requirements.

The School has a Data Retention and Disposal Procedure and a Retention Schedule which provide further guidance on the various types of records the School creates or gathers and how long they are kept for.

If you have any specific queries about how this privacy notice is applied or wish to request that personal data that you no longer believe is relevant is considered for erasure, please contact the School's Privacy Officer.

13. HOW SHOULD YOU PROCESS PERSONAL DATA FOR THE SCHOOL?

Everyone who works for, or on behalf of, the School has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this privacy notice and the School's Data Retention and Disposal Procedure.

The School's Privacy Officer is responsible for reviewing this privacy notice. You should direct any questions in relation to this privacy notice or data protection to the School's Privacy Officer.

- You should only access personal data covered by this privacy notice if you need it for the work you do for, or on behalf of, the School and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling HR if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Personal data should be encrypted before being transferred electronically to authorised external contacts. Please contact the IT Helpdesk for more information on how to do this.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data of others to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area unless in compliance with the law and authorisation of the Privacy Officer.
- You should lock offices, drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from School premises without authorisation from your Line Manager or the Privacy Officer; this includes when permitted to work from home.
- When in paper/physical form, personal data should be shredded and disposed of securely when you have finished with it, or be deleted from the School's systems in accordance with the School's Retention Schedule.
- You should ask for help from the Privacy Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this privacy notice by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

14. HOW TO DEAL WITH DATA BREACHES

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach in accordance with the School's Data Breach Management Procedure. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the School's Privacy Officer immediately and keep any evidence that you have in relation to the breach.

15. SUBJECT ACCESS REQUESTS

Data subjects can make a '**data subject access request**' ('DSAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the School's Privacy Officer who will coordinate a response. The DSARs will be managed in line with the provisions and rules set out under the School's Data Subject Access Request Procedure.

If you would like to make a DSAR in relation to your own personal data, you should make this in writing to the School's Privacy Officer. The School must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a DSAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

16. YOUR DATA SUBJECT RIGHTS

- You have the right to information about what personal data we process, how and on what basis as set out in this privacy notice.
- You have the right to access your own personal data by way of a DSAR (see above).
- You can correct any inaccuracies in your personal data. To do so you should contact the School's Privacy Officer.
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the School's Privacy Officer.
- You have the right to request that we erase your personal data upon termination of your employment with the School. However, please bear in mind that the School may have lawful and necessary reasons to hold on to some data beyond termination of your employment (for example, health and safety and safeguarding information).
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the School's Privacy Officer.
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.

- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- You have the right to be notified of a data security breach concerning your personal data and the School will take all reasonable steps to inform you of such.
- In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the School's Privacy Officer.
- You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

17. DATA ACCURACY AND SECURITY

The School will ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the HR Team of any significant changes to important information such as contact details, bank details etc., held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law), please see the above paragraph for details.

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around the use of technology and devices, and access to School systems. All employees, volunteers, workers and consultants will be made aware of this privacy notice and their duties under Data Protection Law.

18. QUERIES AND COMPLAINTS

Any comments or queries on this privacy notice should be directed to the School's Privacy Officer using the following contact details:

Privacy Officer: DataProtection@johnlyon.org

If an individual believes that the School has not complied with this privacy notice or acted otherwise than in accordance with Data Protection Law, they may wish to notify the School's Privacy Officer. The School 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 regulators.

19. PRIVACY NOTICE DEVELOPMENT AND REVIEW

This procedure is designed to set good practice standards; however, we recognise that best practice develops over time and as such we will update it regularly in the light of experience and because of changes in legislation or our own internal organisation and policies. The procedure will be subject to a comprehensive review on at least an annual basis.

Reviewed by: Chief Operating Officer
Implemented: September 23
Next review: September 24