DATA PROTECTION POLICY

Background

The John Lyon School is a registered Data Controller (No. Z778648X) as part of John Lyon's Foundation.

Data protection is an important legal compliance issue for The John Lyon School (the School). During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties. The manner in which this is done can be found in the School's Privacy Notice. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

The law governing this area changed with the implementation of the General Data Protection Regulation (GDPR). This is an EU Regulation that is directly effective in the UK and throughout the rest of Europe. A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law: this includes specific provisions of relevance to independent schools. In particular, in the context of our safeguarding obligations, the School has a heightened duty to ensure that the personal data of pupils is at all times handled responsibly and securely.

While the law does set out useful legal grounds in this area, in most ways this new law is strengthening the rights of individuals and placing tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and has powers to take action for breaches of the law.

All members of staff at School who are involved in the processing of personal data are obliged to comply with this policy when doing so. It is almost inevitable that accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action. All breaches are investigated and logged – see Appendix 2 for more information.

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. There are also separate rules for the processing of personal data relating to criminal convictions and offences. 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.

Data Protection Lead: Privacy Officer

The School has appointed the Bursar, Mr Michael Gibson, as the Privacy Officer, 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 (please see the Privacy Notice for details).

The 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. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data; and

- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

Meeting the Principles

The School has a number of policies and processes that ensure that these principles are met:

- **Data Protection Policy** – available to staff, governors, parents and others on request. This explains the principles and main responsibilities of the School and is complemented by staff training.
- **Privacy Notice** – available to all data subjects through the School website, making the School's processes and data processing transparent to all data subjects.
- **Data Asset Register** – outlines the lawful basis for retention of data, retention periods, risk management and other checks.
- **Parent Contract**: Terms and Conditions – makes the Privacy Notice and Data Protection Policy available to parents.
- **Annual Staff training** – all staff will be trained in the principles and practical steps of data protection on the first day the academic year. New staff will be trained as part of their induction if beginning out of cycle.
- **Photographic Images Policy** – available to parents in Parent Handbook and linked to IT Policy.
- **IT Policy** including AUP for staff, pupils, governors and visitors – linked directly to Photographic Images Policy and Data Protection Policy
- **Online Safety Policy** – clear guidance for staff in protecting sensitive data about pupils. Linked to IT Policy.

Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under the GDPR (and because of the fact that it can be withdrawn by the data subject) it is generally considered preferable to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the controller. It can be challenged by data subjects and also means the controller is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as the GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School 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.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from requests for access to information. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

Data handling

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

Responsible processing also extends to the creation and generation of new personal data/records, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

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 – please consult Appendix 2 below for details of this process. 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.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the staff member's contract.

Care and data security

More generally, we require all School staff to remain conscious of the data protection principles (see 'The Principles' above), to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

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.

Rights of individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Privacy Officer as soon as possible. Please see Appendix 1, below, for the School's processes for dealing with Subject Access Requests.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Privacy Officer as soon as possible.

Data Security: online and digital

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.

Processing of Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). John Lyon School staff do not process credit/debit card data, such transactions are processed by staff at Harrow School. Harrow School operates strictly within the requirements of PCI DSS. For transactions where the client is not present card details are only accepted over the telephone and are never written down. The member of staff inputs the details directly into the on-line software. Neither school will ever accept card details by email or post. The security of Harrow School's ICT systems is regularly tested to ensure it complies with PCI DSS.

Data Protection: Summary

The GDPR is a good law, recognising that it is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

When handling any data, but particularly personal or sensitive data, a good rule of thumb is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but as a code of useful and sensible considerations to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

Appendix 1: Subject Access Requests

Subject Access Requests: Processing

Checking of identity

We will first check that we have enough information to be sure of your identity. Often we will have no reason to doubt a person's identity, for example, if we have regularly corresponded with them. However, if we have good cause to doubt your identity we can ask you to provide any evidence we reasonably need to confirm your identity. For example, we may ask you for a piece of information held in your records that we would expect you to know, a witnessed copy of your signature or proof of your address.

If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone under the Mental Capacity Act 2005, you must confirm your capacity to act on their behalf and explain how you are entitled to access their information. If you are the parent/guardian of a child in Year 9 or above, we will need to consider whether the child can provide their consent to you acting on their behalf.

Should you make a data subject access request for which you are not the data subject, you must stipulate the basis under the General Data Protection Regulation that you consider makes you entitled to the information.

Collation of information

We will check that we have enough information to find the records you requested. Where a general request is made, we may ask for greater clarity to refine our search to provide the information requested. If we feel we need more information, then we will promptly ask you for this. We will gather any manual or electronically held information (including emails) and identify any information provided by a third party or that identifies a third party.

If we have identified information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information to you unless the other party has provided their consent or it is reasonable to do so without their consent. If the third party objects to the information being disclosed we may seek legal advice on what action we should take.

Before sharing any information that relates to third parties, we will where possible anonymise information that identifies third parties not already known to the individual (e.g. John Lyon School employees), and edit information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document. The GDPR requires us to provide information not documents.

Issuing our response

Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent to you except where you agree, where it is impossible, or where

it would involve undue effort. In these cases, an alternative would be to allow you to view the information on screen at the School.

We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.

Fees

We do not charge a fee for subject access requests under the GDPR, however, if the request for information is manifestly excessive or similar to previous requests, the School may ask you to reconsider, or require a proportionate fee (but only where data protection law allows it).

Timeframe

The School will endeavour to respond to any written requests as soon as is reasonably practicable and in any event within statutory time limits (one month in the case of requests for access to information).

The School will be better able to respond quickly to smaller, targeted requests for information and in some cases will ask for further detail from those making a request, to see if the process can be simplified and therefore processed more quickly. Please note that, as stated above under Fees and in the Privacy Notice, if the request for information is manifestly excessive or similar to previous requests, the School may ask you to reconsider, or require a proportionate fee (but only where data protection law allows it).

Grounds for not complying with a Subject Access Request:

Previous request

If a previous subject access request has been made we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

Exemptions

The Data Protection Act contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. Possible exemptions include: information covered by legal professional privilege, information used for research, historical and statistical purposes, and confidential references given or received by The John Lyon School.

Identification of an Error in Records

If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction. If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

Requests to Stop Processing Data

Under the GDPR, you can object to the School processing your data altogether, in relation to a particular purpose or in a particular way by contacting the Privacy Officer. However, this only applies to certain processing activities and there is a process that you must follow when making such an objection. We must then give you written notice that either we have complied with your request, intend to comply with it or state the extent to which we will comply with it and why. This information will be given to you within 21 days of the School receiving the initial request. Further information on this can be found at https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/

Complaints procedure

Any comments or queries on this policy should be directed to the Bursar, Mr Michael Gibson using the following contact details**:** Michael.Gibson@johnlyon.org or in writing by post to Mr Michael Gibson, The John Lyon School, Middle Road, Harrow on the Hill, HA2 0HN.

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, Miss Katherine Haynes (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.

Template Letter for submitting a Subject Access Request

[Your full address]
[Phone number]
[The date]

The John Lyon School

Dear Sir or Madam,
Subject access request
[Your full name and address and any other details to help identify you and the data you want.]

Please supply the data about me that I am entitled to under data protection law relating to: [give specific details of the data you want, for example:

- my personnel file
- emails between 'person A' and 'person B' (from 1 June 2017 to 1 Sept 2017)
- CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm

If you need any more data from me, or a fee, please let me know as soon as possible. It may be helpful for you to know that data protection law requires you to respond to a request for data within one calendar month.

If you do not normally deal with these requests, please pass this letter to the School's Provacy Officer, or in their absence, another relevant staff member.

Yours faithfully,

[Signature]

Appendix 2: Data Breach Management

In the event of a suspected breach of the Data Protection Act the following is the process that will be followed by the School.

1. Upon the first employee becoming aware of the breach:

The employee immediately reports the matter to the School's Privacy Officer or, in their absence, the Head or a Deputy Head.

2. Initial assessment, containment and recovery – first few hours:

The School will make an initial assessment of the breach, considering the following questions:

- How long has the breach been active?
- What data was involved?
- How far has it got/how widely dispersed is the information?

The School will then seek to contain and recover the information as far as possible, considering the following factors (among others):

- if a cyber breach, involve the School's IT personnel from the outset;
- if human actor(s) are involved, can they be contacted to give reassurances;
- if e.g. Royal Mail, courier, IT or other contractors are involved, can they assist;
- are specialists needed: forensic IT consultants, crisis management PR, legal etc.

3. Ongoing assessment of risk and mitigation – first 72 hours (and initial notification where required):

In the first 72 hours of any data breach being identified, the School will seek to build up a more detailed picture of the risk and reach of the security breach, considering:

- how many have been affected?
- was any sensitive personal data involved – for example health in medical notes, or crime in employment records?
- was financial data involved and/or is there a risk of identify fraud?

The School will consider whether a crime has been committed and therefore whether to involve police or the cyber crime unit. The School would have no hesitation in reporting any matter that they suspected of being a crime.

The School would consider if insurers need notifying, as the breach may amount to a major loss, crime, or possible legal claim.

The School, as part of its assessment, will consider whether the breach would lead to the likely risk of harm to the data subjects and therefore if it:

- is sufficient to require a full or preliminary notification to the ICO; and
- is sufficiently serious to require communication to affected individuals.

When considering reporting to agencies or to individuals the School will assess:

- if not considered to have met the reporting threshold, is this a matter we can document but deal with internally?; or
- if it has met the threshold, what can we usefully tell the ICO and/or individuals at this stage?
- If the School should provide fraud or password advice, offer counselling etc.

4. Ongoing evaluation, monitoring and remediation:

The School will:

- Continue to monitor and assess possible consequences (even if apparently contained).
- Keep the ICO and/or those affected informed as new information becomes available.
- Tell the ICO and/or those affected what we are doing to remediate and improve practice.

The School will also begin the process of internal review, initially considering the following matters:

- How did this happen? What could we have done better?
- Would training or even disciplinary action be justified for staff members?
- Were our policies adequate, and/or adequately followed?
- If our contractors were involved (e.g. systems providers), did they respond adequately? Do we have any remedies against them if not?

5. Record-keeping and putting outcomes into practice:

The School will:

- Keep a full internal record, whether or not the matter was reported or resulted in harm.
- Log this record against wider trends and compare with past incidents.
- Make sure all past outcomes were in fact put into practice.
- Ensure any recommendations made by, or promised to, the ICO are actioned.
- Notify the Charity Commission as an RSI at an appropriate juncture.
- Review policies and ensure regular (or specific, if required) training is actually completed.

Process of Reporting to ICO

Serious breaches will be reported to the ICO using:

- the security breach helpline 0303 123 1113 (open Monday to Friday, 9am to 5pm). Selecting option 3 to speak to staff who will record the breach and give advice; or,
- the security breach notification form, which should be sent to the email address: casework@ico.org.uk; or,
- by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form can be found here: https://ico.org.uk/for-organisations/report-a-breach/

Template Letter for Raising a Concern about Data Management

[Your full address]
[Phone number]
[The date]

The John Lyon School

[Reference number (if provided within the initial response)]

Dear Sir or Madam,

Information rights concern

[Insert your full name and address and any other details such as account number to help identify you]

I am concerned that you have not handled my personal information properly.

[Give details of your concern, explaining clearly and simply what has happened and, where appropriate, the effect it has had on you.]

I understand that before reporting my concern to the Information Commissioner's Office (ICO) I should give you the chance to deal with it.

If, when I receive your response, I would still like to report my concern to the ICO, I will give them a copy of it to consider.

Please send a full response within within one calendar month. If you cannot respond within that timescale, please tell me when you will be able to respond.

If there is anything you would like to discuss, please contact me on the following number *[telephone number]*.

Yours faithfully,

[Signature]