LOCKERS PARK SCHOOL

DATA PROTECTION POLICY

This policy refers to the whole school including boarding and EYFS

Date Last Updated	By...	Date of next review
May 2018	CRW	

Aims

Lockers Park School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

The policy includes all personal data, regardless of whether it is stored in paper or electronic form.

Definitions

Personal data

This refers to any information relating to an identified, or identifiable, individual. This may include the individual's: name (including initials); identification number; location data; online identifier (such as username). It may also include specific factors that relate to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Sensitive personal data

This is data of a higher sensitivity and therefore needs more protection, including information about an individual's: race or ethnicity; political views; religious or philosophical beliefs; trade union membership; genetics; biometrics; health (physical or mental); sex life or sexual orientation.

Processing

This is anything that happens to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. This can happen in both automated and manual form.

Data Subject

This is the identified or identifiable individual whose personal data is held or processed

Data controller

This is the person or organisation that determines the purposes and the means of processing of personal data.

Data processor

This is the person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach

This is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The data controller

Lockers Park processes data relating to parents, pupils, staff, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the Information Commissioner's office (ICO) and will renew this registration as required.

Roles and responsibilities

This policy applies to all staff employed by Lockers Park, and to external organisations or individuals working on our behalf. Members of staff who do not comply with this policy may face disciplinary action.

Headmaster

The headmaster has overall responsibility for ensuring that the school complies with all relevant data protection obligations. He will also act as the data controller on a day-to-day basis.

All staff

Members of staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data
- Contacting the headmaster in the following circumstances:
    - If they have any concerns the policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or gain consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside of the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need any help with contracts or the sharing of personal data with third parties
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

Data protection principles

GDPR is based on data protection principles that Lockers Park must comply with. These principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate, and where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy will set out how the school aims to comply with these principles.

Procedures

Collecting personal data – Lawfulness, fairness and transparency

Lockers Park will only process data in line with one of six legal reasons to do so under the data protection law. These are:

- In order to fulfil a contract with the individual
- So that the school can comply with a legal obligation
- To ensure the vital interests of the individual (e.g. to protect someone's life)
- To enable the school to perform a task in the public interest and carry out its official functions
- For the legitimate interests of the school or a third party
- If the individual (which in the case of the pupils will be the parent/carer) has freely given clear consent

When collecting sensitive personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Individuals are provided with a copy of our Privacy Policy which details our purposes for processing personal data. The Privacy Policy is also on the school website.

Limitation, minimisation and accuracy

The school will only collect personal data for specified, explicit and legitimate reasons.

If the school wants to use personal data for reasons other than those given when first obtained, the school will inform the individuals concerned beforehand and seek consent where necessary.

The staff must only process personal data where necessary in order to fulfil their roles.

When staff no longer need the personal data they hold they must ensure that it is deleted or anonymised.

Sharing personal data

Personal data may be shared when:

- There is an issue with a pupil or parent/carer that puts the safety of the staff at risk
- We need to liaise with other agencies (we will seek consent as necessary)
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils. When doing this we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside of the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

Subject access requests

Individuals have the right to make a subject access request to gain access to personal information that the school holds about them. This includes:

- Access to a copy of the data
- The purposes of the data processing
- The categories of the personal data concerned
- Confirmation that their personal data is being processed
- Who the data has or will be shared with
- How long the data will be stored for

- The source of the data if it is not the individual

Subject access requests must be submitted to the headmaster by email. They should include:

- The name of the individual
- The correspondence address
- The contact number and email address
- Details of the information requested

Any member of staff receiving a subject access request must immediately forward it to the headmaster.

Pupils and subject access requests

Personal data about a child belongs to that child and not the child's parents/carer.

Pupils can make a subject access request for their own personal data provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. This is generally considered to be age 13 and above, although this will depend on both the child and the personal data request, including any relevant circumstances at home.

Parents/carers can make a request for their child's data where the child is not considered mature enough to understand their rights over their own data.

Responding to subject access requests

When responding to subject access requests, the school will follow the procedures set out in its Subject Access Request (SAR) Procedure. This can be found in Appendix 1.

Other data protection rights of the individual

In addition to those elements mentioned above, individuals also have the right to:

- Withdraw consent to processing at any time when consent is needed
- Ask the school to rectify, erase or restrict processing of their personal data , or object to the processing of it
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their data to be transferred to a third party in a structured, commonly used and machine readable format

Individuals should submit any request to exercise these rights to the headmaster. If staff receive a request, they must immediately forward it to the headmaster.

Parental requests to see the educational record

There is no automatic parental right of access to a pupil's educational record in independent schools, but we are likely to provide relevant information on request. Such a request should be made to the headmaster.

Photographs and Videos

Parents will be asked to opt in to the use of their child for school material including marketing elements. This will also include any video footage that may be used.

Data protection by design and default

The school will put measures in place to show we have integrated data protection into all of our data processing activities, including:

- Only processing personal data that is necessary for each specific purpose of processing
- Completing data privacy impact assessments where the school's processing of personal data presents a high risk. All DPIA's will be signed off by the headmaster and reviewed as and when required. A DPIA form can be found in Appendix 2.
- Integrating data protection into internal documents
- Regularly training staff on data protection law
- Regularly conducting reviews and audits to test privacy measures and compliancy
- Maintaining records of our processing activities

Data security and storage of records

The school will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper based records and portable electronic devices that contain personal data are kept under lock and key when not in use
- Papers that contain confidential personal data will not be left anywhere where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. These passwords will be changed at regular intervals
- Where the school needs to share personal data with a third party, the school will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure in Appendix 3. When appropriate, we will report the data breach to the ICO within 72 hours.

Training

Data protection training will form part of the induction process for all staff. Ongoing training will occur in line with any legislation changes that occur. The policy will be reviewed annually.

Appendices:

Appendix 1: Subject Access Request Procedure

Appendix 2: Data Privacy Impact Assessment form

Appendix 3: Personal Data Breach procedure

Data protection policy Appendix 1

Subject Access Request (SAR) procedure

An individual can request details of personal data which is being held about them. The following process should be followed when making an SAR:

- A request in writing detailing the information they wish to see. This should be sent for the headmaster by emailing secretary@lockerspark.herts.sch.uk
- The request will be reviewed by the headmaster and the individual will be contacted if further information is required (e.g. to confirm the identity or authority of the individual)
- Once the headmaster has all the information required an acknowledgement will be sent to the individual confirming receipt of the request and advising that the information requested will be provided within 1 calendar month of the acknowledgement. This may be extended by a further 2 months if the request is complex or numerous. The individual will be advised if this is the case. Where requests are deemed to be manifestly unfounded or excessive the school has the right to refuse to respond. Where this is the case an individual will be provided with an explanation in writing and informed of their right to complain.
- Where information requested identifies third parties, information will be redacted to protect the identity of them, (unless permission has been expressly given by the third party).
- There may be occasions where information is exempt from this process (e.g. if it is legally privileged). Each SAR will be assessed by the headmaster when the request is received.
- The headmaster will liaise with the individual in relation to the delivery of the information when it is ready to be sent
- The information will be provided free of charge
- A log of SAR's received and actions taken will be maintained by the headmaster

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the individual
- Would reveal that the individual is at risk of abuse, where the disclosure of that information would not be in the child's best interest
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning a child
- Is legally privileged

Data protection policy Appendix 2

Data Privacy Impact Assessment (DPIA) form

This form should be completed when a new project is being considered and where changes used are planned to existing practices.

DPIA forms should be completed in liaison with the headmaster who will then sign it off.

Date of assessment	
Completed by	
Name of the process	
Purpose of the process	
Under what legal basis is the information being processed?	
Where does the data come from?	
In which locations does the processing take place?	
Who is impacted by the processing?	
What is the process for deleting the data?	
What risks are there to the data subject?	
What measures are currently in place to protect the data subject and their rights?	
What additional measures will be put in place to ensure all risks are covered?	
Is the risk deemed too high, medium or low?	
Date of next review	

Reviewed and signed off by headmaster:

Data protection policy Appendix 3

Personal Data Breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach or potential breach, the staff member or data processor must immediately inform the headmaster, providing as much information as possible.
- The headmaster will investigate the report, along with the SMT, and determine whether a breach has occurred.
- The headmaster will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members
- The headmaster will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The headmaster will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis.
- The headmaster will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the headmaster will do this via the "report a breach" page of the ICO website within 72 hours. As required the headmaster will set out:
    - A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned
    - The name and contact details of the headmaster
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the headmaster will report as much as he can within 72 hours. The report will explain that there is a delay, the reasons why, and when the headmaster expects to have further information. The headmaster will submit the information as soon as possible.

- The headmaster will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the headmaster will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set pout:
    - The name and contact details of the headmaster
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The headmaster will notify any relevant third parties who can help mitigate the loss to individuals
- The headmaster will document each breach, irrespective of whether it is reported to the ICO. For each breach the record will include: Facts and cause, effects and action taken.
- Records of all breaches will be held by the headmaster within the breach log.
- The SMT will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.