



# DATA PROTECTION POLICY FOR LONDON KOREAN SCHOOL

## 1. Introduction

LONDON KOREAN SCHOOL (LKS) has a responsibility to maintain its records and record keeping systems. It aims to ensure that all personal data collected about members of staff, children, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. When doing this, LKS will take account of the following factors:

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Accessibility of records and record keeping systems.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Definitions

Term	Definition
<b>Personal data</b>	Any information relating to an identified, or identifiable, living individual.  This may include the individual's: <ul style="list-style-type: none"> <li>• Full Name</li> <li>• Location data (i.e. home address)</li> <li>• Contact numbers (i.e. landline and/or mobile number)</li> <li>• Online identifier (i.e. email address)</li> <li>• Names of siblings, if applicable</li> </ul>
<b>Special categories of personal data</b>	Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none"> <li>• <b>Health – physical or mental (e.g. allergies, health issues etc.)</b></li> <li>• <b>Special Educational Needs and Disability (SEND)</b></li> </ul>
<b>Processing</b>	Anything done to personal data, such as collecting, recording,

	organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.  Processing can be automated or manual.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

### 3. The Data Controller

London Korean School processes personal data relating to pupils, parents, staff, support staff, volunteers, trustees, visitors and others, and therefore is a data controller. The controller shall be responsible for, and be able to demonstrate compliance with the data processing principles outlined below (refer to **4. Principles** in this policy).

As LKS is a non-profit organisation, we are exempt from the Information Commissioner's Office (ICO) registration. However we strictly follow the UK GDPR guidance in general.

### 4. Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest or historical research purpose shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest or historical research purpose subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss,

destruction or damage, using appropriate technical or organizational measures.

## 5. Roles and Responsibilities

**5-1.** This policy applies to **all members of staff, support staff and volunteers employed by LKS**, and **trustees**. They are aware of their responsibilities under the UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

### 5-2. Trustees

The Board of Trustees has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

### 5-3. Headteacher

The headteacher acts as the representative of the data controller.

### 5-4. All staff

Staff (including support staff and volunteers) are responsible for:

- Collecting, storing, processing and deleting any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the data controller in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this 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 there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- **All staff, support staff and volunteers are expected to sign a confidentiality statement.**
- Staff must only process personal data where it is necessary in order to do their jobs.
- When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done accordance with Information and Records management Society's toolkit for schools (see [https://issuu.com/irmsbulletin/docs/14049\\_irms\\_school\\_s\\_toolkit\\_2019\\_pr](https://issuu.com/irmsbulletin/docs/14049_irms_school_s_toolkit_2019_pr)).

## 6. Processing Personal Data and Confidentiality within LKS

**6-1.** LKS will only process personal data where we have lawful bases (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can comply with a legal obligation.
- The data needs to be processed to ensure the vital interest of the individuals e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interest of the school.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

**6-2.** Any sensitive personal information which falls under the category of **special categories of personal data** is given special protection and must be held in the utmost confidence.

**6-3.** We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. We also process this data in accordance with the following confidentiality procedures within the school:

- Any information that a child discloses to a member of staff, support staff, volunteers or any adult visiting the school should not be passed on to other colleagues indiscriminately but should only be passed on a "need to know basis".
- Members of staff should not offer children or their parents, blanket or unconditional confidentiality.
- Any information concerning a child's behaviour or conduct that is likely to cause harm to themselves or to others should be passed on to LKS's DSL(Designated Safeguarding Lead) as well as the Headteacher.
- This policy should be shared with every parent and child (at age appropriate level). It should be made clear when and with whom information will be shared.
- Where a child discloses information about physical or sexual abuse, neglect or emotional abuse, the member of staff, support staff, volunteers, trustees or any adult visiting the school must follow the procedures outlined in LKS Safeguarding Children Policy.
- If someone believes that a child may be suffering, or may be at risk of suffering, significant harm, then they should always refer their concerns to the Designated Safeguarding Lead (DSL) who will follow the procedures outlined in LKS Safeguarding Children Policy. LKS will generally seek to discuss any concerns with the family and, where possible, seek their agreement to making any referrals. However, this should only be done where such discussion and agreement-seeking will not place a child at increased risk of significant harm.
- If such disclosed information is to be passed on, the child should be told of this, know who the information will be passed on to and why and who else in the school, or externally, will have access to the information. The child should also be reassured that

they will be offered appropriate ongoing support.

**6-4.** If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

**6-5.** LKS will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.

**6-6.** We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

**6-7.** We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

## **7. Photographic Images and Video Recordings**

- As part of the school activities, we may take photographs and video recordings of children within our school.
- We will obtain written consent from parents/carers for photographs and video recordings to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photographic images and/or video recordings will be used to parents/carers.
- Consent can be refused or withdrawn at any time by writing to the school. At that point, any images of the child will not be used in future publications, however continuing inclusion in publications already in circulation cannot be prevented.
- When using photographs and video recordings in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See LKS Photography Policy for more detailed information on our use of photographic images and video recordings.

## **8. DBS Data**

- All data provided by the DBS will be handled in line with the Data Protection legislation; this includes electronic communications.
- Data provided by the DBS will never be duplicated.

## 9. Data Security and Storage of Records

- Every child has a personal record with their contact details, SEND information, medical information and settling in information. These records are kept in a locked cabinet and are only accessible to the child's key person or class teacher.
- Staff records and details are kept locked in a secure storage.
- Staff are aware that when they are discussing a child, confidentiality should take priority. This will always be the case regardless of talking with parents or other staff in the setting.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords that are at least 8 characters long containing letter and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

## 10. 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.

## 11. Personal Data Breaches

- LKS 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 based on **guidance on personal data breaches**<sup>1</sup> produced by the Information Commissioner's Office (ICO).

---

<sup>1</sup> <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/#:~:text=If%20the%20breach%20is%20likely,internal%20reporting%20procedures%20in%20place>

## **12. Training**

- All staff and trustees are provided with data protection training as part of their induction process. They are also regularly updated with any changes made in LKS Data Protection Policy.
- Data protection will form part of continuing professional development, where changes to legislation, guidance, or the school's processes and policy make it necessary.

## **13. Key Points**

- Staff, support staff, volunteers and trustees will not discuss individual children, other than for the purposes of curriculum planning/group management, with people other than the parents/carers or key person of that child;
- Information given by parents/carers will not be passed on to other adults without permission;
- Issues to do with the employment of staff, whether paid or unpaid, will remain confidential to the people directly involved with making personnel decisions;
- The use of social network internet sites should not be used to discuss any school issues.

New Policy, November 2023

Updated 28 November 2023

This policy will be reviewed and updated where necessary.



## Confidentiality Statement

Confidentiality, whether personal, financial or of any other category must be respected at all times.

Information on the personal history of all children will be kept securely. It will only be accessed when necessary and only then by authorised personnel, who will ensure that none of the information is revealed to any unauthorised third party.

To meet the needs of all the children in our care it is important to share information with parents and one another in order to support the child's development. It may also be necessary, in some circumstances, for the school to seek help and advice from outside professionals. If this action is taken, the parents' permission will normally be obtained first.

All members of staff will agree to support and respect the school's GDPR/Data Protection Policy and will sign a statement to indicate their agreement.

## Confidentiality Agreement

During the course of your work you will be privy to confidential information about staff members, volunteers, trustees and children in our care and their families. You may need to discuss confidential issues with other staff members, or professionals from outside agencies, in order to effectively carry out your work. Any information and knowledge will be on a 'need to know' basis and will be kept confidential.

At no time are you to disclose confidential information to any unauthorised third party, either verbally, by email or by the use of social media/internet networks.

Failure to comply with our GDPR/Data Protection Policy and this statement will result in disciplinary action,

Signed: \_\_\_\_\_

Name: \_\_\_\_\_  
(please print)

Date: \_\_\_\_\_