Lea Nursery School

Headteacher: Linda Stay
Chair of Governors: David MacIsaac

Data Protection Policy

This policy is applicable to all regardless of gender, sexuality, religious belief or none, culture, ethnicity, ability or disability, individuals with protected characteristics and those with none; it does not determine to discriminate against any individual whilst ensuring the smooth operation of our school.

Approved by Governing Body:	
Date:	Autumn 2021 (Checked LJS 20/4/21)
Review Date:	Autumn 2022

Wexham Road, Slough, SL2 5JW
Tel: 01753 536492
E-mail: post@lea-nursery.slough.sch.uk
Website: www. lea-nursery.slough.sch.uk

Contents

1. Overview

1.1. The Lea Nursery School (hereafter 'the school'), takes the security and privacy of personal data seriously. We need to gather and use information or 'data' about our stakeholders as part of our business and to manage our relationship with them. The School intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the United Kingdom General Data Protection Regulation ('UK GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2. This policy applies to current and former employees, governors, volunteers, apprentices, and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside any contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to personal data.

1.3. The School has separate Privacy Notices in place in respect of job applicants, pupils, parents, and other categories of data subject. A copy of these can be obtained from the school website or the school office.

1.4. The School has measures in place to protect the security of personal data in accordance with our ***Data Security Policy***. A copy of this can be obtained from the school office.

1.5. The School will hold data in accordance with our ***Data Retention Policy and Schedule***. A copy of this can be obtained from the school office. We will only hold data for as long as necessary for the purposes for which we collected it.

1.6. The School is a 'Data Controller' for the purposes of data protection data. This means that we determine the purpose and means of the processing of personal data.

1.7. This policy explains how the School will hold and process personal data. It also explains your obligations when obtaining, handling, processing, or storing personal data in the course of working for, or on behalf of, the School.

1.8. This policy 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.

2. Legislation and Guidance

2.1. This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance provided by the Information Commissioners Office (ICO) on the UK GDPR and the ICO's Code of Practice for subject access requests. If any conflict arises between those laws and this policy, the School intends to comply with the 2018 Act and the UK GDPR.

2.2. It also reflects the ICO's code of practice for the use of surveillance cameras (CCTV).

3. Definitions

3.1. The terms in this document have the meanings as set out in Article 4 of the GDPR unless amended by the Act.

3.2. For clarity, the following have been reproduced:

> ***'personal data'*** means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
>
> '***special category personal data***' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of

genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

'***processing***' means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

'***data controller***' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

'***data processor***' means a person, other than an employee of the data controller, who processes the data on behalf of the data controller.

'***data subject***' means a person whose personal data is held or processed.

4. The Data Controller

4.1. The school processes personal information relating to staff, pupils, parents, volunteers, visitors, and other stakeholders and is a Data Controller.

4.2. The School delegates the responsibility of Data Controller to the Data Controller's Representative (see Section 5 below)

4.3. The School is registered as a data controller with the Information Commissioner's Office – registration number Z8647020 and renews this registration annually or as otherwise legally required

5. Roles and Responsibilities

5.1. Governing Board

5.1.1. The Governing Board has overall responsibility for ensuring that the school complies with its obligations under the UK GDPR and the Data Protection Act 2018

5.2. Data Protection Officer

5.2.1. The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

5.2.2. The DPO will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

5.2.3. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

5.2.4. Our DPO is The Schools People (See Contact details below)

5.3. The Headteacher

5.3.1. The Headteacher acts as the Data Controller's representative on a day-to-day basis. In their absence, the Deputy Head will undertake the role.

5.3.2. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

5.4. All Staff

5.4.1. All staff are responsible for:

- ensuring that they collect and store any personal data in accordance with this policy.
- keeping the school informed of any changes to their personal data, such as a change of address.
- Contacting the DPO 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 they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Prior to engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

6.1. The UK GDPR is based on data protection principles that the school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, 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

6.2. This policy sets out how the school aims to comply with these principles.

7. Lawfulness, Fairness and Transparency

7.1. Lawfulness, Fairness and Transparency

7.1.1. We will only process general category personal data where we a ‘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 interests of the individual 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

7.2. Where the School ***is not*** operating in its capacity as a public authority, for example for the purposes of after-school activities not tied to curriculum, the lawful basis for that processing will be legitimate interest.

7.3. The school can process personal data for these purposes without knowledge or consent.

7.4. The School will not use personal data for an unrelated purpose without disclosing the intent, providing the lawful basis for the processing, and seeking consent if necessary.

7.5. Whenever personal data is collected from individuals, they will be provided with the relevant information including details of the data collected and how it is collected, stored, and shared, via a Privacy Notice (sometimes called a Fair Processing Notice) as required by the UK GDPR and the Data Protection Act (2018).

7.6. Special Category Data

7.6.1. In processing 'special categories' of personal data, we will also meet one of the special category conditions set out in the UK GDPR, in that

- The individual or person with the lawful authority to exercise consent on an individual has given explicit consent
- The data needs to be processed to ensure the vital interest of the individual where they are physically or legally incapable of giving consent
- The data has manifestly made public by the individual e.g., on social media
- Processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

7.6.2. Where relevant a condition specified in Schedule 1 of the Data Protection Act 2018 (see Appendix1: **Appropriate Policy Document**)

7.7. Criminal Convictions

7.7.1. The school may use information relating to criminal convictions where the law allows us to do so. It is envisaged the school will hold information about criminal convictions if information about criminal convictions comes to light as a

result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during a stakeholder's relationship with the School. Information about criminal convictions and offences will be used in the following ways:

- To ensure employee suitability to work
- For safeguarding purposes

7.7.2. Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect an individual's interests (or someone else's interests) and they are not capable of giving your consent, or where the information has already been made public.

7.8. Limitation, Minimisation and Accuracy

7.8.1. The School 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.

7.8.2. If the school wants 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 to further processing where necessary.

7.8.3. Staff must only access and process personal data where it is necessary in order for them to do their jobs.

7.8.4. When the School no longer needs the personal data it holds, it must be stored, deleted, or anonymised in accordance with the ***Data Retention Policy and Schedule***

8. Accountability & Record Keeping

8.1. The Schools Data Protection Officer is The Schools People, who can be contacted by emailing **DPOService@schoolspeople**.co.uk or calling **01773 851 078**

8.2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the School's other data protection-related policies, and compliance with the UK GDPR and other applicable data protection legislation.

8.3. The School shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the School, its Data Protection Officer, and any applicable third-party data processors:
- The purposes for which the School collects holds, and processes personal data:
- Details of the categories of personal data collected, held and processed by the School, and the categories of data subject to which that personal data relates:
- Details of any transfers of personal data outside the UK, including all mechanisms and security safeguards:
- Details of how long personal data will be retained by the School (please refer to the School's ***Data Retention Policy & Schedule***); and
- Detailed descriptions of all technical and organisational measures taken by the School to ensure the security of personal data.

9. Automated Decision Making

9.1. Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

9.2. The School does not envisage that any decisions will be taken about data subjects using automated means. If this position changes the School will update this policy and the relevant ***Privacy Notices*** accordingly

10. Sharing Personal Data

10.1. The school is obliged to share personal data in order to meet contractual or statutory obligations. Examples of organisations with whom the School regularly share personal data with include, but are not limited to:

- Department for Education
- The Local Authority
- Ofsted
- Disclosure and Barring Service
- HMRC
- Teachers' Pension Service
- Local Government Pension Service

10.2. The School will also share personal data with law enforcement, government bodies and the local authority where legally required to, and to help them to respond to an emergency situation that affects any of our staff or pupils, including:

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

10.3. Suppliers and/or contractors also require personal data to provide services to the School. For example:

- Payroll
- HR
- Occupational Health services
- Sims for Schools
- Medigold Health

10.4. The School requires those companies to keep personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process personal data for the lawful purpose for which it has been shared and in accordance with our instructions.

10.5. The School will: -

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with current data protection legislation
- Establish a data-sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share in line with UK GDPR, the Data Protection Act (2018), and our Policies
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

11. Transferring Data Outside The UK

11.1. We do not routinely share data with organisations outside the UK.

11.2. Personal data will not be outside the United Kingdom (UK) unless such transfer complies with the UK GDPR. This means that we cannot transfer any personal data outside the UK unless:

- The Secretary of State has decided that another country or international organisation ensures an adequate level of protection for personal data
- The transfer is subject to appropriate safeguards under the UK GDPR
- One of the derogations in the UK GDPR applies (including if an individual explicitly consents to the proposed transfer).

12. Data Security

12.1. Everyone who works for, or on behalf of, the School has responsibility for ensuring data is collected, stored, and handled appropriately, in line with this policy and the School's Data Security and Data Retention policies.

12.2. Data Security - Organisational Measures

- the School shall ensure that the following measures are taken concerning the collection, holding, and processing of personal data:
- all staff, volunteers, contractors, service providers or other parties working on behalf of the School shall be made fully aware of their individual responsibilities and the School's responsibilities under the UK GDPR and this Policy, and shall have free access to a copy of this Policy
- only those working for or on behalf of the School that require access to, and use of personal data to carry out their assigned duties shall have access to personal data held by the School
- those working for or on behalf of the School who engage with the handling personal data will be appropriately trained to do so and adequately supervised
- those working for or on behalf of the School shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise
- methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed
- all personal data held by the School shall be reviewed periodically, as set out in the School's ***Data Retention Policy.***

12.3. Data Security -Technological Measures

12.3.1. The School shall ensure that the following measures are taken concerning IT and information security:

- The School requires that any passwords used to access personal data shall have a minimum of 8 characters, composed of a mixture of upper- and lower-case characters, numbers, and symbols. Passwords are not expected to be changed regularly, but users will be expected to change their password when instructed by the School.
- Passwords should not be written down or shared between any staff or other parties working for or on behalf of the School, irrespective of seniority or function. If a password is forgotten, it must be reset using the applicable method.
- All software (including, but not limited to, applications and operating systems) shall be kept up to date. The School's IT company shall be responsible for installing security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any School-owned computer or device without authorisation.

12.4. Contravention of these rules may be treated as a disciplinary matter.

12.5. Data Security - Storage

12.5.1. The School shall ensure that the following measures are taken concerning the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption
- All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar
- All personal data relating to the operations of the School, stored electronically, should be backed up regularly
- Where any member of staff stores personal data on a mobile device (whether that be a computer, tablet, phone, or any other device) then that member of staff must abide by the School's ***Acceptable Use Policy***. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information

12.6. Data Security – Disposal

12.6.1. The School shall ensure that the following measures are taken concerning the disposal of personal data:

- When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted or disposed of in accordance with the ***Data Retention Policy and Schedule***.

- 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. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.
- We may also use a third-party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with current data protection law and provides a Certificate of Destruction for our records.
- For more information, please refer to the ***Data Retention Policy & Schedule***

12.7. Data Security – Use of Personal data

12.7.1. The School shall ensure that the following measures are taken concerning the use of personal data:

- No personal data may be shared informally and if an employee, volunteer, processor, or other party working for or on behalf of the School requires access to any personal data that they do not already have access to. Such access should be formally requested from the relevant Business Manager.
- Personal data must always be handled with care and should not be left unattended or on view to unauthorised persons at any time
- If personal data is being viewed on a computer screen and the computer is to be left unattended, the user must lock the computer and screen before leaving it; and
- Where personal data held by the School is used for marketing purposes, appropriate checks to ensure consents for such processing are in place must be carried out before the data is used.

12.8. Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with the School's Disciplinary Procedure.

13. Personal Data Breaches

13.1. The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected or actual data breach, we will follow the procedure set out in our ***Data Security Policy and Breach Procedure***.

13.2. When appropriate, we will report the data breach to the ICO within 72 hours. Examples of such breaches may include, but are not limited to:

13.3. See the ***Data Security Policy and Breach Procedure*** for more information

14. Subject Access Requests (SARs)

14.1. Individuals have the right to make a 'Subject Access Request' ('SAR') to gain access to personal information that the School holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data held
- Who the data has been, or will be, shared with?

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

14.2. A SAR may be made in writing or verbally, through traditional channels of communication or through Social Media. If a SAR request is received it should forward it immediately to the Data Controllers Representative who will liaise with the Data Protection Officer and coordinate a response.

14.3. A SAR does not have to contain the words Subject Access Request. Any communication, whether written or verbal, that requests access to personal data should be treated as a possible SAR. Refer to the ***Subject Access Request Policy and Procedure*** for further information.

14.4. Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

14.5. There is no fee for making a SAR. However, if a request is unfounded or excessive the School may charge a reasonable administrative fee or refuse to respond to the request

14.6. 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 dismissal.

14.7. The School has defined a process for handling SARs and other data subject requests. Please refer to the ***Subject Access Request Policy & Procedure***

15. Other Data Subject Rights

15.1. Data Subjects have the right to:

- access their own personal data by way of a subject access request (see 14.1 above)
- correct any inaccuracies in their personal data
- request that we erase their 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
- restrict the processing of their personal data in certain circumstances
- object to data processing where the School is relying on a legitimate interest to do so, and the Data Subject feels their rights and interests outweigh our own
- object to the processing of data for direct marketing.
- ask the School to transfer personal data to another data controller (in certain circumstances).
- with some exceptions, not to be subjected to automated decision-making. The School does not use automated decision making.
- be notified of a data security breach in certain situations
- complain to the Information Commissioner.

16. CCTV

16.1. The School use CCTV in various locations around the school site. We will adhere to the ICO's code of practice for the use of CCTV.

16.2. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

16.3. For more information about the school's use of CCTV please refer to ***CCTV Policy***

16.4. Any enquiries about the CCTV system should be directed to the Headteacher

17. Photographs and Videos

17.1. As part of School activities, we may take photographs and record images of individuals within the School

17.2. Staff must not take images of children unless they have:

- A legitimate reason for doing so
- Permission to do so

17.3. The School will obtain written consent from parents/carers, for photographs and videos to be taken of pupils and for use in communication, marketing, and promotional materials. When requesting consent, we will clearly explain how the photograph and/or video will be used to the parent/carer. Uses may include:

- Within the School on displays, notice boards and in newsletters
- Outside of School by external agencies such as the School photographer, newspapers, or marketing literature
- Online on our School website or social media pages

17.4. When using photographs and videos staff must not accompany them with any other personal information about the child, to ensure they cannot be identified.

17.5. Consent to use pupil images may be refused or withdrawn at any time. If consent is withdrawn, photographs and/or video must be withdrawn and deleted as soon as possible.

18. Data Protection by Design and Default

18.1. We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

18.2. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

18.3. Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

18.4. Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

18.5. Integrating data protection into internal documents including this policy, any related policies and privacy notices

18.6. Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance

18.7. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

18.8. Maintaining records of our processing activities, including:

18.9. For the benefit of data subjects, making available the name and contact details of the school, the DPO and all information we are required to share about how we use and process their personal data (via our Privacy Notices)

18.10. For all personal data that we hold, maintaining an internal record of the data processing activity (RoPA) detailing the data processed, the category of data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

19. Data Protection Impact Assessments

19.1. The School shall carry out Data Protection Impact Assessments for all new projects and/or new uses of personal data which involve the use of new technologies/new service providers and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

19.2. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed
- The purpose(s) for which personal data is to be used
- The School's objectives
- How personal data is to be used
- The parties (internal and/or external) who are to be consulted
- The necessity and proportionality of the data processing related to the purpose(s) for which it is being processed
- Risks posed to data subjects
- Risks posed both within and to the School and
- Proposed measures to minimise and handle identified risks.

20. Training and Awareness

20.1. School staff and governors are provided with data protection training as part of their induction process.

20.2. Data Protection forms part of continuing professional development, where changes to legislation or the school's processes make it necessary.

21. Monitoring Arrangements

21.1. The School's Data Protection Officer and the Data Controller's Representative (School Business Manager) are responsible for reviewing this policy and updating the Governing Body on the School's data protection responsibilities and any risks in relation to the processing of data. Any questions in relation to this policy or data protection should be directed to these persons.

21.2. The Headteacher/Data Controller's Representative (Office Manager), together with the Data Protection Officer, will check that the school complies with this policy by reviewing school records, policies, and procedures annually.

21.3. This policy will be reviewed and updated as and when necessary, in relation to any amendments to Data Protection legislation or guidance, or any internal concerns resulting from policy violations, data breaches, or on an annual basis.

21.4. At every review, the policy will be shared with the Governing Body.

22. Contacts

22.1. Questions or concerns about how the School processes personal, please contact the school in the first instance.

22.2. If you have concerns that we are not able to resolve to your satisfaction you can contact our Data Protection Officer at the email address below.

Alternatively, you may register a concern with the UK's data protection regulator - the Information Commissioner's Office, by following this link https://ico.org.uk/make-a-complaint/

Contacts

Data Controller: Lea Nursery School, Wexham Road, Slough, SL2 5JW
Data Controller's Representative: Linda Stay, Headteacher.

Email: Head@lea-nursery.slough.sch.uk

Data Protection Officer: The Schools People - Dee Whitmore.

Email: DPOService@Schoolspeople.co.uk

23. Links with Other Policies

23.1. This Data Protection Policy is linked to:

- Appropriate Policy Document (Appendix 1)
- Data Retention Policy and Schedule
- Data Security Policy and Breach Procedure
- Record of Processing Data Breach Activity
- Subject Assess Request Policy
- CCTV Policy
- Privacy Notice for Parents
- Privacy Notice for Pupils
- Privacy Notice for Job Applicants
- Privacy Notice for Governors
- Privacy Notice for Volunteers
- The Freedom of Information Policy and Scheme

Appendix 1: Appropriate Policy Document

For use when relying on specified conditions for the processing of special categories of personal data, and personal data relating to criminal convictions and offences

1. Introduction

1.1. This is the 'Appropriate Policy Document' required when Lea Nursery School seeks to rely on any of the conditions specified in Schedule 1 to the Data Protection Act 2018, for the processing of special category and criminal convictions personal data.

1.2. The content of this Appropriate Policy Document meets the requirements of paragraph 39 of Schedule 1 of the Data Protection Act (2018), in that it –

- explains the School's procedures for securing compliance with the principles in Article 5 of the UK General Data Protection Regulation ('UK GDPR') - principles relating to the processing of personal data, in connection with the processing of personal data in reliance on the condition in question; and
- explains the School's policies as regards the retention and erasure of personal data processed in reliance on the condition, indicating how long such personal data is likely to be retained.

1.3. Under paragraph 40(1) of Schedule 1 of the DPA (2018), where the School processes personal data in reliance on a condition described in paragraph 38 of Schedule 1, they will, during the relevant period[1]

- retain the appropriate policy document,
- review and (if appropriate) update it from time to time, and
- make it available to the Information Commissioner, on request, without charge

2. Description of Data Processes

2.1. As part of its statutory and business functions, the School processes special category data related to stakeholders, including staff, governors and volunteers, job applicants, pupils, and parents/carers. This includes where relevant, information about health, disability and wellbeing, ethnicity, trade union membership, religious or philosophical beliefs, biometric data. Further information about this processing can be found in the relevant Privacy Notices.

2.2. Processing for reasons of substantial public interest relates to the data the School receives, obtains, or creates to fulfil our statutory obligations. For example, this may be related to the safeguarding of pupils, supporting staff with a particular disability or medical condition, for equal opportunities monitoring, safeguarding, etc.

2.3. A record of our processing activities is kept under Article 30 of the UK GDPR.

3. Schedule 1 Condition for Processing

3.1. The School processes special category data for the following purposes in Part 1 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 1: Employment, social security, and social protection.

[1] The 'relevant period' begins when the data is collected and ends no less than 6 months following cessation of the processing

3.2. The School may process special category data for the following purposes in Part 2 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 6: Statutory, etc. purposes.
- Paragraph 8: Equality of opportunity and treatment.
- Paragraph 16: Support for individuals with a particular disability or medical condition
- Paragraph 17: Counselling
- Paragraph 18: Safeguarding of children and individuals at risk
- Paragraph 20: Insurance
- Paragraph 21: Occupational Pensions

4. Criminal Offence Data

4.1. The School processes criminal offence data for the following purposes in parts 1 and 2 of Schedule 1 of the Data Protection Act (2018).

- Paragraph 1 – employment, social security, and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 18 (1) Safeguarding of Children and individuals at risk

5. Securing Compliance with the Data Protection Principles

5.1. The School's procedures for complying with Article 5 of the GDPR: Data Protection Principles are as follows:

Principle A: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The School will:

- ensure that personal data is only processed where at least one of the conditions in Schedule 1 is met or the data subject has given their explicit consent for the processing.
- only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent (provision of privacy notices).
- where necessary carry out Data Protection Impact Assessments to ensure proposed processing is carried out fairly.

Principle B: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The School will:

- only collect personal data for specified, explicit and legitimate purposes and will inform data subjects what those purposes are through the provision of privacy notices.

- not use personal data for purposes that are incompatible with the purposes for which it was collected.
- before personal data is used for a new purpose that is compatible, the School will inform the data subject.

Principle C: Personal data shall be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.

The School will:

- only collect the minimum personal data needed for the purpose for which it is collected.
- ensure the data is adequate and relevant to the purpose for which it is collected.
- apply Data Protection Impact Assessments to ensure proposed processing is not excessive.
- Where personal data is provided to or obtained by the School but is not relevant to a stated purpose, it will be erased.

Principle D: Personal data shall be accurate and, where necessary, kept up to date.

The School will ensure that:

- personal data is accurate and kept up to date as necessary.
- when notified of inaccuracies personal data is corrected.
- Where the School become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, every reasonable step will be taken to ensure that data is erased or rectified without delay. If the School decides not to either erase or rectify it, for example, because the lawful basis relied upon to process the data means these rights don't apply, the decision not to erase will be documented.

Principle E: Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The School will ensure that:

- personal data will only be kept in identifiable form only as long as is necessary for the purposes for which it is collected unless otherwise required by law.
- when no longer needed, personal data shall be securely deleted or anonymised.
- personal data is held and disposed of in line with the School's Data Retention Policy and Schedule.

Principle F: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The School will ensure that:

- there are appropriate organisational and technical measures in place to protect personal data.
- data is processed in accordance with its Data Handling and Classification Procedure and Data Security Policy and Procedure.

6. Accountability Principle

6.1. Under GDPR Article 5(2), the School is responsible for and must be able to demonstrate compliance with the principles listed above.

6.2. The School has appointed a Data Protection Officer in accordance with Article 37 of the UK GDPR. The DPO provides independent advice and monitoring of personal data handling and has access to report to the highest management level.

6.3. The School will:

- ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner on request (Ropa).
- carry out a Data Protection Impact Assessment for any high-risk personal data processing and consult the Information Commissioner if appropriate.
- have in place internal policies and procedures to ensure that personal data is collected, used, or handled only in a way that is compliant with data protection law.
- Policies for Retention and Erasure of Personal Data
- The School will ensure, where special category or criminal convictions personal data is processed, that:
- there is a Record of Processing Activities (ROPA), and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data.
- where special category or criminal convictions personal data is no longer required for the purpose for which it was collected, it will be securely deleted or rendered permanently anonymous in accordance with the School's Data Retention Policy and Schedule.
- data subjects receive a Privacy Notice (sometimes called a fair processing notice) detailing how their data will be handled, including the period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period.

7. Additional Special Category Processing

7.1. The School processes special category personal data in other instances where there is not a requirement to keep an Appropriate Policy Document. Our processing of such data is in accordance with data protection legislation and respects the rights and freedoms of the data subjects.

7.2. The School will provide clear and transparent information about why personal data is processed including the lawful basis for processing in stakeholder Privacy Notices. Copies of Privacy Notices are available from the office.