www.slough.gov.uk
Slough Borough Council

Taking pride in our communities and town

The Lea Nursery School
Wexham Road, Slough, Berks
SL2 5JW

Data Protection Policy

Approved by Governing Body:	
Date:	Spring 2020
Review Date:	Autumn 2021

Contents

1. Overview

1.1 The Lea Nursery School (hereafter 'the school'), takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('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 your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your personal data.

1.3 The School has separate Privacy Notices in place in respect of job applicants, pupils, parents, suppliers 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 your 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. 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 your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.7 This policy explains how the School will hold and process your information. It explains your rights as a data subject. 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 GDPR and the DPA 2018. It is based on guidance provided by the Information Commissioners Office (ICO) on the 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 GDPR.

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

3. Definitions

Term	Definition
Personal Data	Information relating to a living individual, who can be identified from that data on its own, or when taken together with other information likely to come into our possession It includes any expressions of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymized data This may include the individuals: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Category Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed or is alleged to have committed, an offence • Criminal convictions We may hold and use any of these special categories of your personal data in accordance with the law.

Processing	Any action relating to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The person whose personal data is held or processed
Data Controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data Processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The Data Controller

4.1 The school processes personal information relating to staff, pupils, parents, volunteers, visitors and other stakeholders and is, therefore, 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 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 Assistant 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 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 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

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

7. Lawful Bases for Processing Personal Data

7.1 Lawfulness, Fairness and Transparency

7.1.1 We will only process general category personal data where we have one of 6 '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
- The individual has freely given clear consent

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

7.1.3 The school will not use personal data for an unrelated purpose without disclosing the intent and providing the legal basis for the processing.

7.2 Special Category Data

7.2.1 In processing 'special categories' of personal data, we will also meet one of the special category conditions set out in the GDPR and Data Protection Act 2018.

- 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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

7.3 Criminal Convictions

7.3.1 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 employment with us. Information about criminal convictions and offences will be used in the following ways:

- To ensure employee suitability to work
- For safeguarding purposes

7.3.2 Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect your interests (or someone else's

interests) and you are not capable of giving your consent, or where you have already made the information public.

7.3.3 Whenever we first collect personal data from individuals, we will provide them with the relevant information including details of the data we collect and how it is collected, stored and shared, via a Privacy Notice (sometimes called a Fair Processing Notice) as required by the GDPR and the Data Protection Act 2018

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

7.4 Limitation, Minimisation and Accuracy

7.4.1 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.

7.4.2 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.

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

7.4.4 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. Examples of when the school might process your personal data

8.1 The school must process personal data in various situations during recruitment, employment (or engagement) and even following termination of employment (or engagement). For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- to train you and reviewing your performance;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability;
- to monitor diversity and equal opportunities;
- to monitor and protect the security (including network security) of the School, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, and stakeholders;

- to pay you and provide pension and other benefits in accordance with the contract between us;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions;
- to monitoring compliance by you, us and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us;
- to answer questions from insurers in respect of any insurance policies which relate to you;
- to manage the School and plan for the future;
- for the prevention and detection of fraud or other criminal offences;
- to defend the School in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- and for any other reason which we may notify you of from time to time.

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. The School may use automated decision-making in the following circumstances:
Where you have been notified of an automated decision and been given 21 days to request a reconsideration.

- Where it is necessary to meet our obligations under your employment contract and ensure that appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

9.2 If the School makes an automated decision on the basis of any particularly sensitive personal information, it must have either your explicit written consent or it must be justified in the public interest, and it must also put in place appropriate measures to safeguard your rights.

9.3 You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless there is a lawful basis for doing so and you have been notified.

9.4 The school does not envisage that any decisions will be taken about you using automated means, however, we will notify you in writing if this position changes.

10. Sharing your Personal Data

10.1 The school is obliged to share your personal data in order to meet obligations under our contract with you or to meet our statutory obligations. Examples of organisations with whom we share your personal data 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 We will also share personal data with law enforcement, government bodies and the local authority where we are 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 Our suppliers and/or contractors also require personal data to provide services to our staff. For example:

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

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

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 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 EEA

11.1 We do not routinely share data with organisations outside the EEA. Where this may be necessary, e.g. where a former employee has emigrated and/or applied to work outside the EEA, data may be transferred to the new employee with explicit consent from the former employee and with appropriate safeguards.

11.2 We will not transfer personal data outside the European Economic Area (EEA) unless such transfer complies with the GDPR. This means that we cannot transfer any personal data outside the EEA unless:

11.3 The EU Commission has decided that another country or international organisation ensures an adequate level of protection for personal data

11.4 One of the derogations in the GDPR applies (including if an individual explicitly consents to the proposed transfer).

12 How You Should Process Personal Data on behalf of the School

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

- only access personal data covered by this policy if you need it for the work you do for, or on behalf of the School and only if you are authorised to do so.
- only use the data for the specified lawful purpose for which it was obtained.
- not share personal data informally.
- keep personal data secure and not share it with unauthorised people.
- regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- use strong passwords.
- lock your computer screens when not at your desk.
- encrypted personal data before transferring it electronically to authorised external contacts.
- not save personal data to your own personal computers or other devices.
- not transfer personal data outside the European Economic Area except in compliance with the law and with the authorisation of the Headteacher.
- lock drawers and filing cabinets. Staff should not leave documents with personal data lying about.
- not take personal data away from School premises without authorisation from the Headteacher.
- shred and securely disposed of personal data in accordance with the Data Retention Policy and Schedule when you the School has no further use for it.
- ask for help from our Data Protection Officer/Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

12.2 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.

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

13. Data Breaches

13.1 The School has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we

must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

13.2 If you are aware of a data breach you must contact the Headteacher and/or the DPO immediately and keep any evidence you have in relation to the breach.

13.3 For further information and instruction please refer to the Data Security Policy and Breach Procedure

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 A form is available to staff, Governors, and other stakeholders who work for or on behalf of the school who wish to make a SAR in relation to their own personal data. Use of the form is not compulsory. The school must accept a SAR in any written or verbal form. The school may, however, contact the requester for further information if necessary. At a minimum a SAR must contain:

- The requester's full legal name
- Correspondence address
- Contact number and email address
- Details of the information requested

Please refer to the Subject Access Request Policy and Procedure for further information

14.5 Children and Subject Access Requests

14.5.1 Under data protection legislation, pupils have the right to request access to information about then that we hold. Personal data belongs to the data subject, and in the case of the personal data of a child regardless of their age the rights in relation to that personal data are theirs and not

those of their parents. Parents, in most cases, do not have automatic rights to the personal data of their child.

14.5.2 However, there are circumstances where a parent can request the personal data of their child without requiring the consent of the child. This will depend on the maturity of the child and whether the School is confident that the child can understand their rights. Generally, in the UK, where a child is under 13 years of age, they are deemed not to be sufficiently mature as to understand their rights of access and a parent may request access to their personal data on their behalf.

14.6 Responding to Subject Access Requests

14.6.1 When responding to requests, we:

- May ask the individual to provide 2 forms of identification if we are not confident about the requester's identity
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of a valid Subject Access Request. A request is not considered valid until we have confirmed the identity of the requester and their entitlement to the requested data
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

14.6.2 We will not disclose the information if it:

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

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

14.6.4 A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

14.6.5 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

15. Other Data Subject Rights

15.1 You have the right to:

- access your own personal data by way of a subject access request (see 14.1 above).
- correct any inaccuracies in your personal data.
- request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected.

- restrict the processing of your personal data in certain circumstances
- object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own.
- object to the processing of your data for direct marketing.
- ask the school to transfer your personal data to another data controller.
- 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 concerning your personal data in certain situations

15.2 In most situations we will not rely solely on consent as a lawful ground to process your data. If we do request your consent to the processing of your personal data for a specific purpose and there is no other lawful basis on which the school may relay for that processing, you have the right not to consent or to withdraw your consent later.

15.3 complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

16. CCTV

16.1 We 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 can 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:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- 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)
- 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)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- 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
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
- 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)
- 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 Security and Storage of Records

19.1 We 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, 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 office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off-site, staff must sign it in and out from the school office
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals

19.2 Staff, Governors or other stakeholders who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Staff Information Systems Code of Conduct)

19.3 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 (see section 11)

20 Disposal of Records

20.1 Personal data that is no longer needed will be disposed of securely in accordance with our Data Retention Policy.

20.2 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.

20.3 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.

20.4 For more information please refer to the Data Retention Policy

21 Personal Data Breaches

21.1 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 set out in our Data Security Policy and Breach Procedure.

21.2 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:

- Safeguarding information being made available to an unauthorised person
- Theft of a school laptop containing non-encrypted personal data about pupils

21.3 See the Data Security Policy and Breach Procedure for more information

22. Training

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

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

23. Contacts

23.1 If you have any questions or concerns about how we process information or wish to exercise any data protection rights, please contact the school in the first instance.

23.2 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.

23.3 Alternatively, you can 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/

23.4 Contact Details

Data Controller: Lea Nursery School, Wexham Road, Slough, SL2 5JW
Data Controller's Representative: Nikki Elsmore-Cary, Headteacher.

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

Data Protection Officer: The Schools People - Dee Whitmore.

Email: DPOService@Schoolspeople.co.uk

24. Changes to this Privacy Notice

24.1 This Policy will be reviewed on a yearly basis or as necessary in relation to changes in Data Protection legislation.

24.2 We reserve the right to update this Policy at any time, and we will provide you with a new policy when we make any substantial updates.

25 Links with Other Policies

25.1 This Data Protection Policy is linked to:

- Data Retention Policy and Schedule
- Data Security Policy and Breach Procedure
- Record of Processing 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