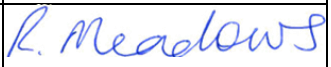
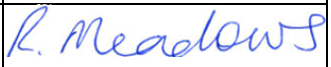
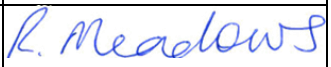
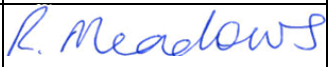
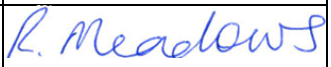
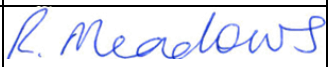


Sladefield Infant School
Data Protection Policy

Policy Version	Revisions	Date Approved	Signed by Governor	Signed by Headteacher
2.0	12.7.9 Video conferencing 12.7.10 Online Resources	24.03.26		
2.1	Remove references to EU/EEA Insert references to UKGDPR 9.1 update to IRMS 2019 12.7.9 Insert reference to ICO Children's Code 17.4.2 Insert references to SCCs	24.03.26		
2.2	5.2 Update DPIA references 6.1 Insert reference to previous employers 8.1 Update standards regarding data accuracy 12.6 Update bullet points referencing data security 12.7.1 update display/publication of images guidance 14.3 amend data breach reporting process	24.03.26		
2.3	5.11 Insert reference to adults providing consent on behalf of children 8.2 Insert data collection requirement 12.7.7 Insert portable storage devices prohibited 19. Insert section detailing information rights	24.03.26		
2.4	5.11, 5.12 revision of adults acting behalf of children 9.2, 9.4 Insert retention and disposal process 12.4.2, 12.4.3 – Insert staff authorisation process for new processing 19.4 Insert form of authority for information rights	24.03.26		
2.5	Insert references to Data Use and Access Act (DUAA) 5.1.55 Insert recognised legitimate interests statement 12.7.11 Insert Artificial Intelligence statement 12.9 – 12.12 Insert use of children's images statements 19.17 insert reasonable and proportionate searches statement 22 Insert Complaints section	24.03.26		

CONTENTS

1 INTRODUCTION 4

2 ABOUT THIS POLICY 4

3 DEFINITION OF DATA PROTECTION TERMS 4

4 DATA PROTECTION PRINCIPLES 5

5 FAIR, LAWFUL AND TRANSPARENT PROCESSING 6

6 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES 7

7 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING 7

8 ACCURATE AND UP-TO-DATE DATA 8

9 RETENTION AND DISPOSAL 8

10 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS 8

11 NOTIFYING DATA SUBJECTS 10

12 DATA SECURITY 11

13 REGISTER OF PROCESSING ACTIVITIES 14

14 REGISTER OF BREACHES 14

15 DATA PROTECTION OFFICER 15

16 USING DATA PROCESSORS 15

17 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK 16

18 DISCLOSURE AND SHARING OF PERSONAL INFORMATION 16

19 RIGHTS OF DATA SUBJECTS 17

20 REQUESTS FOR INFORMATION 19

21 CONTACTING THE DATA PROTECTION OFFICER 19

22 CHANGES TO THIS POLICY 20

1 INTRODUCTION

1.1 Sladefield Infant collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory responsibilities.

1.2 School staff are obliged to comply with this Policy when processing Personal Data on the school's behalf. Any breach of this Policy by school staff may result in disciplinary or other action.

2 ABOUT THIS POLICY

2.1 The school holds Personal Data about current, past and prospective pupils, parents, employees and others with whom the school communicates. Personal Data may be recorded on paper, stored electronically, visual media or other formats.

2.2 This Policy and other documents referred to in it set out the basis on which the school will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

2.3 This Policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 The Data Protection Officer is responsible for supporting the school with compliance with the Relevant Data Protection Laws and with this Policy. That post is held by Services4Schools Ltd. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer. The Data Protection Officer can be contacted at DPO@sladefield.bham.sch.uk or by writing to Sladefield Infant School, Bamville Road, Birmingham, B8 2TJ.

3 DEFINITION OF DATA PROTECTION TERMS

3.1 In this Policy, the functions of the school are the provision of education to its pupils, the safeguarding of children in its care, the undertaking of pastoral support, necessary business and administrative tasks, community work and similar activities associated with that provision. References to the school 'carrying out its functions' or similar are references to these activities.

3.2 References to 'we' are references to the school.

3.3 **Data Subjects** means identified or identifiable natural (living) persons whose Personal Data the school holds. These may be pupils, parents/carers, staff, governors, volunteers, visitors etc. This Policy also refers to Data Subjects as 'individuals.'

3.4 **Data Controllers** are the people who, or organisations which, determine the purposes for which any Personal Data are processed, including the means of the processing.

The school is the Data Controller of all Personal Data used for carrying out its functions.

3.5 **School Staff** are, for the purposes of this Policy, those of our employees whose work involves processing Personal Data and any governors or volunteers appointed to support or represent the school. School staff must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

3.6 **Data Processors** include any person or organisation, who is not a member of school staff, which processes Personal Data on the school's behalf, including any external suppliers that handle Personal Data on the school's behalf.

3.7 **Privacy Notices** are documents explaining to Data Subjects how their data will be used by the school.

3.8 **Personal Data** means any information relating to an identified or identifiable natural (living) person; 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.

3.9 **Personal Data Breach** means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data the school is responsible for.

3.10 **Pseudonymisation** means the processing of Personal Data so that it can no longer be attributed to a specific person without the use of additional information. This additional information (or key) must be kept separately and is subject to measures to ensure that the identity of the Data Subject remains protected.

3.11 **Relevant Data Protection Law** means the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Data Use and Access Act 2025, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and all applicable laws and regulations relating to the processing of Personal Data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.

3.12 **Special Categories of Personal Data** (formerly known as 'sensitive Personal Data') includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of Personal Data can only be processed under strict conditions.

4 DATA PROTECTION PRINCIPLES

4.1 Anyone processing Personal Data for, or on behalf of, the school must comply with the principles of good practice contained in Relevant Data Protection Law. These principles state that Personal Data must be:

4.1.1 processed fairly, lawfully and transparently;

4.1.2 processed for specified, limited and legitimate purposes and in an appropriate way;

4.1.3 adequate, relevant and not excessive for the purposes for which they are

processed;

4.1.4 accurate and, where necessary, kept up to date;

4.1.5 not kept longer than necessary for the intended purpose of processing; and

4.1.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The school will keep a record of all Data Processing activities and must be able to demonstrate its compliance with these principles and with the wider requirements of Relevant Data Protection Law.

5 FAIR, LAWFUL AND TRANSPARENT PROCESSING

5.1 For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in Relevant Data Protection Law. These include, but are not limited to:

5.1.1 the individual's explicit consent to the processing for one or more specified purposes;

5.1.2 that the processing is necessary for the performance of a contract with the individual or for the compliance with a legal obligation to which the school is subject;

5.1.3 that the processing is in the public interest; or

5.1.4 that the processing is in the legitimate interest of the school or relevant third parties to which the data are disclosed, so long as this is balanced with the rights and freedoms of the individual.

5.1.5 That processing is in the recognised legitimate interests of the school or an organisation undertaking official duties

5.2 Where a change to a process, or introduction of a new process involving the use of large volumes of Data Processing, that is likely to pose a high risk to individuals' rights, the school will carry out an appropriate Data Protection Impact Assessment (DPIA) in line with Article 35 of UKGDPR.

5.3 *Special Categories of Personal Data*

5.4 When Special Categories of Personal Data are being processed, the individual's explicit consent to processing of those data must be obtained unless the processing:

5.4.1 is necessary for the purposes of carrying out the obligations and exercising specific rights of the school or of the individual in the field of employment and social security and social protection law;

5.4.2 is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;

5.4.3 relates to Personal Data which are manifestly made public by the individual;

5.4.4 is necessary for reasons of substantial public interest; or

5.4.5 is necessary to protect the vital interests of the individual.

5.5 Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where UK law states that processing must take place.

5.5.1 This is undertaken as part of the pre-employment check process (DBS) for all staff employed by the school, or where it is necessary to perform such a check as required by safeguarding regulation.

5.6 *Consent of adults and organisations*

5.7 Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the school) or a positive action demonstrating consent. Any requests that the school makes for consent must be in clear language.

5.8 An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the school requests consent.

5.9 *Consent of children and young people*

5.10 Where consent is the lawful basis of processing pupil information, consent must be obtained from an appropriate parent, carer, legal guardian, or official body acting on behalf of the child.

5.11 We will not seek consent from children directly, as all children who attend Sladefield Infant School will be under the age of 16.

5.12 Where an adult is providing consent on behalf of a child, reasonable measures should have been taken to determine the individual is acting in interests of the child's information rights.

6 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES

6.1 In the course of carrying out its functions, the school may collect and process the Personal Data set out in its information asset register. This may include data we receive directly from an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, parents/carers, other schools, the local authority or other public bodies, previous employers, recruitment agencies, service providers, professional advisers and others).

6.2 The school will only process Personal Data for the specific purposes set out in Privacy Notices, consent forms or for any other purposes specifically permitted by Relevant Data Protection Law.

7 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the individual.

7.2 If a member of staff has any doubt as to whether any processing exceeds the purposes for which that data was originally collected, they should notify the Data Protection

Officer.

8 ACCURATE AND UP-TO-DATE DATA

8.1 We will ensure that Personal Data we hold are accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8.2 Parents and staff will be encouraged, at least annually, to review the currency and accuracy of information held by the school through the performance of a data collection exercise.

8.3 It is the responsibility of all staff to ensure that Personal Data they handle is accurate and kept up to date. If staff become aware that personal data is incorrect or requires updating, they should make this change in school systems, or notify the relevant person who has access to make this change without delay.

8.4 All staff must, as a minimum check that any Personal Data that they provide to the school in connection with their employment is accurate and up to date. They must also inform the school of any changes to their Personal Data that they have provided, e.g. change of address, either at the time of appointment or subsequently.

9 RETENTION AND DISPOSAL

9.1 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which are no longer required.

9.2 The school has a Records Management Policy and Retention Schedule which provides guidance on appropriate timescales for retaining certain records which contain Personal Data.

9.3 If a member of staff has any doubt as to whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected, they should seek advice from the Data Protection Officer.

9.4 Records that have exceeded the advised retention period should be disposed of in a secure manner. A log of disposals should be maintained to inform when and how sets of records have been destroyed.

10 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS

10.1 We are committed to upholding the rights of individuals to access Personal Data the school holds on them.

10.2 We will process all Personal Data in line with individuals' rights, in particular their rights to:

10.2.1 be informed, in a manner which is concise, transparent, intelligible and easily accessible and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;

10.2.2 receive confirmation as to whether your Personal Data is being processed by us;

10.2.3 access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. School employees who receive a written request should forward it to the Headteacher and the Data Protection Officer immediately;

10.2.4 have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the school (see also Paragraph 8);

10.2.5 restrict processing of data if one of the following circumstances applies:

a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the Personal Data;

b) the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;

c) the controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

d) the Data Subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the Data Subject.

10.2.6 Where processing has been restricted, as above, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest and the Data Subject shall be informed.

10.2.7 Where processing is restricted under one of the grounds in Paragraph 10.2.5, the data shall only be processed with the individual's consent or in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

10.2.8 An individual who has obtained restriction of processing under Paragraph 10.2.5 shall be informed by the school before the restriction of processing is lifted.

10.2.9 Receive data concerning the individual, which they have provided to the school and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the school.

10.2.10 Object to Data Processing on grounds relating to their particular situation unless the school demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and

10.2.11 Not to be subject to a decision based solely on automated decision-making and profiling which produces legal effects concerning them or similarly

significantly affects them, unless the decision is based on the individual's explicit consent.

10.3 It is the responsibility of all staff to ensure that any request by an individual under Paragraph 10.1 is brought to the attention of the Data Protection Officer without undue delay.

10.4 The school may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.

10.5 The school shall provide information on action taken on a request under Paragraph 10.1 to the individual within one month of receipt of the request unless the school deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.

10.6 If a request under Paragraph 10.2 is unfounded or excessive, the school may charge a reasonable fee for providing the information or refuse the request.

10.7 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

10.7.1 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

10.7.2 We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

10.8 Our employees will refer a request to the Headteacher and the Data Protection Officer. Employees should not be bullied into disclosing personal information.

11 NOTIFYING DATA SUBJECTS

11.1 If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

11.1.1 the identity and contact details for the school and its Data Protection Officer;

11.1.2 the purpose or purposes for which we intend to process those Personal Data;

11.1.3 the types of third parties, if any, with which we will share or to which we will disclose those Personal Data; and

11.1.4 the means, if any, by which individuals can limit our use and sharing of their Personal Data.

11.2 If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information in Paragraph 11.1 above at the following times:

11.2.1 within one month of receiving the Personal Data;

11.2.2 if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;

11.2.3 if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

11.3 A notification in the form of a Privacy Notice will be in writing or via a link to our website, unless the individual requests an oral notification.

11.4 We will also inform individuals whose Personal Data we process that the school is the Data Controller with regard to those data and who the Data Protection Officer is.

12 DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

12.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if they agree to comply with those procedures and policies, or if they put in place adequate measures.

12.3 School staff will be issued with details of their obligations in relation to security of Personal Data.

12.4 All school staff must:

12.4.1 assist the school in upholding individuals' Data Protection rights;

12.4.2 Seek authorisation from the Headteacher, Chair of Governors or Data Protection Officer before using Personal Data for a purpose that is not already authorised;

12.4.3 Seek authorisation from Headteacher, relevant member of SLT, or Data Protection Officer before sharing Personal Data externally for a purpose that is not already authorised;

12.4.4 notify the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches in accordance with Paragraph 12.5;

12.4.5 comply with the standards set out in the school's ICT and Internet Acceptable Use Policy, Confidentiality Policy and Safeguarding Policy;

12.4.6 comply at all times with the terms of any agreements with the school and with their responsibilities under Relevant Data Protection Law;

12.4.7 satisfy the school, within a reasonable period following request, of their compliance with the provisions of Paragraph 12.4.6.

12.5 The Data Protection Officer, in collaboration with the school, will notify the Information Commissioner's Office of any Personal Data Breaches without undue delay.

12.6 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

12.6.1 **Confidentiality:** only people who are authorised to use the data can access them. Information, or records containing personal data should not be shared

with individuals or organisations outside of school, unless there has been prior authorisation, or there is a statutory requirement to do so;

12.6.2 **Integrity:** Personal Data should be accurate and suitable for the purpose for which they are processed;

12.6.3 **Availability:** authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the school's approved systems instead of on individual computers, tablets or other media. Staff should consider whether data is stored on a system, or location that permits relevant staff to access the information they need.

12.7 Security procedures include:

12.7.1 **IT Equipment:** Staff must ensure they have read the school's ICT and Internet Acceptable Use Policy before using school equipment. Screens and monitors should be positioned to prevent the display of confidential information to passers-by and pupils in classrooms. Staff must ensure they log off from their computers, tablets or other devices when left unattended.

12.7.2 **Building Security and Entry controls:** All visitors are required to sign in using appropriate systems. Any unauthorised person seen on the school's premises should be reported to the Office Manager.

12.7.3 **Secure lockable storage:** Rooms, desks, cupboards and filing cabinets should be kept locked when unattended if they are used to store any confidential information (personal information is always considered confidential).

12.7.4 **Appropriate Sharing and Verbal Disclosure:** When providing personal information verbally, particularly by telephone, it is most important that the individual's identity is verified before any information is disclosed and that conversations occur in a space where information cannot be overheard. Voicemails and messages should not include personal data. Where walky-talky systems are used in school, a protocol for appropriate operation will be made available to staff. Pupil data should not be broadcast over walky-talky channels.

12.7.5 **Methods of disposal:** Paper documents containing personal information should be shredded when they are no longer needed (in line with the schools retention periods). Digital storage devices should be handed into relevant staff at the school to be securely destroyed when they are no longer required. A record of disposals should be maintained by the School Business Manager.

12.7.6 **Personal Data on display:** All Personal Data displayed in the school's buildings will be limited to what is necessary and pseudonymised where appropriate. If Personal Data is displayed externally, then consent should be sought prior to publication.

12.7.7 **Electronic Transport/Transfer of Personal Data:** School staff will use only approved methods to transport or transfer data as detailed in the school's ICT policy. The use of removeable storage devices such as portable hardrives and memory sticks is prohibited. Records containing personal data must not be transferred to staff personal accounts or devices without prior

approval from SLT.

12.7.8 **Photographs and Digital Images:** (including video). We use photographs and digital images for a variety of purposes across the school, these include, but are not limited to:

- Capturing development and progress in learning
- School prospectuses and other publications focussed on promoting the school
- Online meetings and videoconferencing
- Assemblies and celebration events
- Sports day
- School performances
- Social Media
- Trips and residential outings

12.7.9 **Use of Online resources**: Where the school employs the use of mobile apps, cloud-based software or other online resources to aid the delivery of teaching and learning, appropriate checks concerning data protection and ICO Children's Code compliance of suppliers will be undertaken prior to use. The Data Protection Officer should be consulted if the sharing pupil or staff data is necessary for the use of such resources (this can include the registration and management of user accounts, or the supply of pupil data to support progress analysis and impact).

12.7.10 **Video Conferencing**: If videoconferencing technologies are used to support meetings or the delivery of blended/remote learning. The Headteacher should approve this use in the first instance. Staff should first consider any implications for the operation of school safeguarding practices when using video conferencing. Guidance is available for all staff on using video conferencing to support teaching and learning.

12.7.11 **Artificial Intelligence:** Where technologies planned for use in school make use of AI and generative AI, these will be risk assessed prior to implementation to ensure data protection compliance. This includes resources and systems used in the delivery of the curriculum and teaching and learning (where pupil data is required), the transcription of meetings, lessons or other live events, and in support of operational management of the school (in administration systems). Advice should be sought from the DPO before AI is used for the purposes of profiling or automated decision making. Special categories of personal data should not be processed using open or generative AI tools.

12.8 Where images of children or staff are published externally, displayed in in public areas, or made available online via publication on the school's website, parental consent will always be sought before images are published.

12.9 Where consent is required in relation to a pupil's image, we will request it from their parent/carer.

12.10 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will take

reasonable steps to cease using the image as part of our marketing and promotional materials.

12.11 Any photographs or videos taken by parents/carers at school events for their own personal use are not covered by data protection law. However, for safeguarding reasons, parents and attendees of publicly accessible school events, should be notified about the appropriate use of such images. This should include notices or announcements explaining that images taken by attendees should not be shared publicly – particularly on social media where accounts are not private.

12.12 For other purposes, however, consent to use people's images may not be required.

12.13 The school shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement Data Protection principles and to integrate the necessary safeguards into processing activities.

12.14 The school shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed.

13 REGISTER OF PROCESSING ACTIVITIES

13.1 The school must maintain an accurate and up-to-date Information Asset Register of processing activities carried out by the school.

13.2 The school must record the following information for each processing activity:

13.2.1 the contact details for the school and its Data Protection Officer;

13.2.2 the purpose or purposes for which the processing activity has occurred;

13.2.3 descriptions of the categories of individuals involved in the processing activity;

13.2.4 descriptions of the categories of Personal Data involved in the processing activity;

13.2.5 descriptions of the categories of recipients of the Personal Data involved in the processing activity;

13.2.6 details of any transfers to third parties, including documentation of the transfer mechanism safeguards in place;

13.2.7 retention schedules;

13.2.8 descriptions of technical and organisational security measures in place relating to the processing activity.

13.3 It is the responsibility of all staff, to notify the Data Protection Officer of any changes that affect the use of Personal Data to ensure that the register of processing activities is accurate and kept up to date.

14 REGISTER OF BREACHES

14.1 The school must maintain an accurate and up-to-date register of all Personal Data

Breaches.

14.2 Staff must take all reasonable steps to minimise the risk of a personal data breach. However, where a data breach does occur, it is important that staff are open and honest about it so that it can be managed quickly.

14.3 If anyone causes, or becomes aware of a Data Protection breach they must inform the Headteacher and Data Protection Officer immediately. This should be done by using the email address DPO@sladefield.bham.sch.uk

14.4 Breaches that occur at school will normally be investigated by the Data Protection Officer and the SBM, or Headteacher. However, if this would create a conflict of interest, the investigation will be completed by the DPO and a representative of the schools Governing Board. Breaches that occur elsewhere within the organisation, or which are caused by a data processor, will also be investigated by the DPO and the Headteacher.

15 DATA PROTECTION OFFICER

15.1 The Data Protection Officer is responsible for supporting the school in compliance with Relevant Data Protection Law and with this Policy. The Data Protection Officer reports to the school's Headteacher and Governing Board but, fulfils their Data Protection functions independently.

15.2 The Data Protection Officer for the school is provided by Services4Schools Ltd and can be contacted at DPO@sladefield.bham.sch.uk or by writing to Sladefield Infant School, Bamville Road, Birmingham, B8 2TJ. Please address letters: **For the attention of the Data Protection Officer.**

15.3 Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

15.4 Where a Personal Data Breach has occurred, it will be for the Data Protection Officer to decide whether, under the circumstances and in accordance with Relevant Data Protection Law, the individual concerned must be informed of the breach.

16 USING DATA PROCESSORS

16.1 The school retains the right to engage by written contract any person or organisation, who is not a member of school staff, to process Personal Data on our behalf.

16.2 Data Processors must:

16.2.1 assist the school in upholding individuals' Data Protection rights;

16.2.2 only act in accordance with the school's instructions and authorisation;

16.2.3 maintain a written record of processing activities carried out on behalf of the school and provide this to the school within [a reasonable period] following request;

16.2.4 notify the school of Personal Data Breaches without undue delay and maintain a register of breaches in accordance with Paragraph 13;

16.2.5 comply at all times with the terms of any agreements with the school and with their responsibilities under Relevant Data Protection Law;

16.2.6 satisfy the school, within a reasonable period following request, of their compliance with the provisions of Paragraph 12.4.6.

17 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

17.1 Individuals have particular rights with regard to transfers of their Personal Data outside the UK. Circumstances in which the school may need to transfer data outside the UK might include use of IT services hosted overseas, arrangement and administration of school trips and cultural exchange projects.

17.2 Subject to the requirements in Paragraph 12.1 above, Personal Data we hold may also be processed by staff operating outside the UK who work for us or for one of our suppliers. Those staff may be engaged, among other things, in the processing of payment details and the provision of support services.

17.3 We may transfer any Personal Data we hold to a country outside the UK provided that:

17.3.1 the transfer to the country or countries in question is permitted by Relevant Data Protection Law; and

17.3.2 any transfer to a country or countries outside the UK is subject the escalation procedure under Paragraph 17.4.

17.4 Before a transfer of Personal Data is made outside the UK, the following safeguards must be provided to ensure that the rights of Data Subjects and effective legal remedies for Data Subjects are available:

17.4.1 confirmation by implementing act by the European Commission of the adequacy of the level of protection afforded by the relevant third country;

17.4.2 standard contractual clauses (SCCs) in accordance with Relevant Data Protection Law must be included in relevant documentation;

17.4.3 ensuring explicit consent is given by the Data Subject to the proposed transfer after having been informed of the possible risks of such transfer;

17.4.4 confirmation that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject;

17.4.5 confirmation that the transfer is necessary for important reasons of public interest;

17.4.6 the Data Protection Officer must authorise the transfer.

18 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

18.1 We may share Personal Data we hold with staff within the school where this is necessary to support teaching and learning, or safeguarding responsibilities.

18.2 We may also disclose Personal Data we hold to third parties:

18.2.1 if we are under a duty to disclose or share an individual's Personal Data in order to comply with any legal obligation;

18.2.2 in order to enforce or apply any contract with the individual or other agreements; or

18.2.3 to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.

18.3 We may also share Personal Data we hold with selected third parties for the purposes set out in the school's Information Asset Register

19 RIGHTS OF DATA SUBJECTS

19.1 We are committed to upholding individuals' rights under data protection law.

19.2 It is important to understand that not all of these rights apply at all times. However, we will ensure all requests to exercise a right are always considered fairly and lawfully.

19.3 We may need to ask for identification from the person making the request before we act upon it.

19.4 Where another individual is exercising information rights on behalf of a data subject, the school will take all reasonable steps to ensure a request is authorised. This will include obtaining a signed form of authority, or where an adult is acting on behalf of child, assessing that the request is made in the interests of the data subject.

19.5 Right to be informed

19.6 People have the right to be informed about what personal data we collect about them and how we use it. We will uphold this right by:

19.7 providing data subjects with the relevant privacy notice at the time we collect their personal data, unless this information has already been given to them or it would be otherwise unreasonable to provide it.

19.8 Privacy Notices will be published on our school website.

19.9 Right of access (subject access)

19.10 People have the right to access their personal data. We will uphold this right by:

19.11 providing information on our websites and Privacy Notices about how to make a subject access request;

19.12 Ensuring staff are able to recognise such a request

19.13 Maintaining a clear process for the handling of information requests

19.14 Regularly reviewing the storage of records containing personal data to minimise data retention and limit the time required for responded to requests;

19.15 Appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported; and

19.16 Clarifying requests as appropriate to confirm which records are to be considered

19.17 Undertaking reasonable and proportionate searches to identify records which contain personal data in the scope of requests

19.18 Reporting requests to the Data Protection Officer without delay

19.19 **Right to rectification**

19.20 People have the right to have their personal data corrected if it is inaccurate, or completed if it is incomplete. We will uphold this right by:

19.21 conducting regular data-checking exercises to give people the opportunity to identify inaccurate data;

19.22 ensuring staff are able to recognise a request to amend personal data;

19.23 Reporting requests to the Data Protection Officer without delay

19.24 **Right to erasure**

19.25 People have the right to have their personal data erased in certain circumstances. We will uphold this right by:

19.26 ensuring staff are able to recognise a request to erase personal data; and

19.27 Reporting requests to the Data Protection Officer without delay

19.28 **Right to restrict processing**

19.29 People have the right to request that we limit how we use their data in certain circumstances. We will uphold this right by:

19.30 ensuring staff are able to recognise a request to restrict processing; and

19.31 Reporting requests to the Data Protection Officer without delay.

19.32 **Right to data portability**

19.33 People have the right to obtain and reuse their personal data across different services by copying or transferring it between systems in a secure way. We will uphold this right by:

19.34 ensuring staff are able to recognise a request for data portability; and

19.35 Reporting requests to the Data Protection Officer without delay

19.36 **Right to object**

19.37 People have the right to object to the processing of their personal data in certain circumstances. We will uphold this right by:

19.38 ensuring staff are able to recognise a request for objecting to processing;

19.39 Responding in a timely manner to request to withdraw or amend consent; and

19.40 Reporting requests to the Data Protection Officer without delay.

19.41 **Rights related to automated decision-making, including profiling**

19.42 People have the right not to be subject to a decision based solely on automated processing, including profiling, which has a significant affect upon them. We will uphold this right by:

19.43 informing people, as part of our privacy notices, about any processing activity that uses automated decision-making and/or profiling;

19.44 completing a data protection impact assessment for any processing activity that is based solely on automated processing, including profiling, and implementing any agreed actions that arise from any such assessment (see section 13);

19.45 ensuring staff are able to recognise a request made under this right;

19.46 appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported; and

19.47 Reporting requests to the Data Protection Officer without delay

19.48 **Parental requests to see the educational record**

19.49 Parents, or those with parental responsibility, can request to access to their child's educational record (which includes most information about a pupil). The academy should make this information available within 15 school days of receipt of a written request.

19.50 Where it is not clear that a request relates solely to accessing educational records, advice should be sought from the DPO prior to disclosure.

20 REQUESTS FOR INFORMATION

20.1 Requests for information may take the following forms:

20.1.1 Requests for education records.

20.1.2 Freedom of information requests.

20.1.3 Subject access requests.

20.1.4 An order from a Court, or a Solicitor to the High Court

20.2 If a person makes a request for information under the Freedom of Information Act, then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the school context may be that information relates to other people, is confidential or legally privileged. If a freedom of information request is made and there are any concerns about disclosing information, then the Data Protection Officer should be contacted.

21 CONTACTING THE DATA PROTECTION OFFICER

21.1 You can contact the DPO directly via:

Email: DPO@sladefield.bham.sch.uk

By Post: Data Protection Officer
Sladefield Infant School
Bamville Road
Birmingham
B8 2TJ

22 COMPLAINTS

22.1 If you have a complaint about how your personal data has been handled by Sladefield Infant School, you should contact the Data Protection Officer in the first instance.

22.2 This policy does not outline the process for complaints and concerns which are directly related to the processing of personal data. Please see the school's Complaints policy if you have a complaint or concern which relates to another matter: https://www.slfield.bham.sch.uk/policies

22.3 Complaints or concerns which relate to data protection or information rights should be submitted in writing to DPO@sladefield.bham.sch.uk

22.4 The Data Protection Officer will conduct an internal review into your complaint respond to you within a calendar month.

22.5 If you are unsatisfied with the response the School has provided, you have the right to contact the Information Commissioners Office. You can do this online at: https://ico.org.uk/make-a-complaint/your-personal-information-concerns/

23 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time. This Policy will be published on the school's website.