PATCHAM INFANT SCHOOL

Our Vision

We dream, we aspire, we thrive.

Powerful learning for life.

DATA PROTECTION POLICY

Data Protection Officer: **Data Protection Education Ltd.**

Telephone: 0800 0862018

Email: dpo@dataprotection.education

CONTENTS

October 2019

The effectiveness of this policy will be monitored by the Governing Body.

Review – statutory requirement of every 2 years.

SCOPE

This policy reflects Patcham Infant School's commitment to the General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018, enacted from 23rd May 2018.

This policy covers the processing of personal data wholly or partly by automated means and the processing of personal data (other than by automated means) which form part of a filing system or are intended to form part of a filing system.

This policy is designed to set out the ways in which personal data of staff, governors, pupils, parents, legal guardians, carers and other relevant individuals is processed fairly and lawfully.

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

A list of important defined terms in the GDPR can be found on the back pages of the policy.

AIMS

Our school aims to ensure that all personal data collected about staff, pupils, parents, legal guardians, carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

THE DATA CONTROLLER

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others and, therefore, is a data controller.

INFORMATION COMMISSIONER'S OFFICE

As we are the Data Controller, we are regulated by the Information Commissioner's Officer. We are registered as a Data Controller with the ICO and will renew this registration annually, or as otherwise legally required.

ROLES AND RESPONSIBILITIES

This policy applies to **all** staff employed by our school and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer

Our named Data Protection Officer is: Data Protection Education and can be contacted at: dpo@dataprotection.education.

We will ensure the following:

- The Data Protection Officer is involved properly and in a timely manner, in all issues relating to the protection of personal data
- Support given to the Data Protection Officer in performing the responsibilities outlined below, by providing resources necessary to carry out those tasks and access to personal data and processing operations:
  - Report directly to the school Business Manager or Headteacher when necessary
  - Be available for contact by data subjects with regard to all issues related to processing of their personal data and to the exercise of their rights under this regulation
  - Bound by secrecy or confidentiality concerning the performance of his or her tasks.

Data Protection Manager

The Data Protection Manager is Mrs Amanda Breeds, School Business Manager, who is responsible for monitoring and reviewing this policy in collaboration with the Headteacher. The Data Protection Manager is the first point of contact within the school for individuals whose data the school processes and will liaise directly with the Data Protection Officer.

Headteacher

The Headteacher acts as the representative of the Data Controller on a day-to-day basis.

All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Data Protection Manager 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 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
- Whenever they are 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.

COMMITMENT

This policy sets out our commitment to GDPR and the implementation of a data protection by design approach. We will refer to documents and guidance from the Information Commissioner's Office and the Department for Education in relation to GDPR and data processing. This includes:

- Creation and maintenance of a data protection working group
- Assigning responsibility to an individual within the school
- Appointing a suitably qualified Data Protection Officer
- Development and maintenance of a GDPR project
- Ensuring that all staff are trained in data protection and take responsibility for the collection, processing, storage and destruction of data
- A lawful basis for processing is documented for all processing activity
- Principles relating to processing of personal data are adhered to
- The rights of data subjects are respected
- Risks to the rights of data subjects are assessed and mitigated for all large-scale and new processing
- Regular independent reviews of processing activity and processing documentation are carried out
- 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 techniques (the DPO will advise on this process)
- Organisational and technical measures are implemented to protect data
- Data breaches impacting on the rights and freedoms of data subjects will be reported to the ICO.

DATA PRINCIPLES

We are committed to the 6 principles relating to processing of personal data, in that personal data will be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject
- **Collected for specific, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving

purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

- **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**
- **Accurate and, where necessary, kept up to date;** every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;** personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical measures required by the GDPR, in order to safeguard the rights and freedoms of individuals
- **Processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

Personal data and sensitive personal data must not be used other than for specific purposes. The data subject should always know that their data is being processed and the purpose. This information is provided in our Privacy Notices.

DATA SUBJECT'S RIGHTS

We support the rights of data subjects (or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to be informed
- Right to be fair and transparent processing
- Right of access
- Right of rectification
- Rights to erasure (the 'rights to be forgotten')
- Right to restrict processing
- Right to be notified of erasure, rectification or restriction
- Right of data portability
- Right to object to processing
- Right to object to processing for the purposes of direct marketing
- Right to object to processing the scientific, historical or statistical purposes
- Right to not be evaluated on the basis of automated processing
- Right to withdraw consent at any time
- Right to be notified about a data breach
- Right to be an effective judicial remedy against a supervisory authority
- Right to lodge a complaint with supervisory authority

- Right to an effective judicial remedy against a controller or processor
- Right to compensation

We shall maintain procedures, policies and notices to ensure that data subjects are informed about their rights.

LAWFUL PROCESSING

We will only process 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 that **vital interests** of the individual, eg to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given, **clear** consent. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. It will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn at any time.

Special categories of personal data will not be processed unless a specific lawful basis listed in Article 9 of the GDPR applies.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

LIMITATION, MINIMISATION AND ACCURACY

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons for the individuals when we first collect their data.

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

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This

will be done in accordance with the guidance on retention periods and disposal or records outlined by the Information and Records Management Society (IRMS).

DATA SHARING

Data will be shared with third parties only where a lawful basis exists.

Where data is shared with third-party processors, they will only process data with our explicit instructions (either contractual or through a data sharing agreement) and shall not hold or process the data for any other purpose. The minimum data required for the processing task will be provided for the processing. Any third-party processors, where contracts or data sharing agreements are required for the processing to take place will be required to provide evidence of their commitment to GDPR compliance.

Where we have a legal obligation to share information with law enforcement, agencies and government bodies for legitimate purposes relating to criminal justice and taxation we will do so.

We will share information if there is an issue that jeopardises the safety or security of staff, pupils or school visitors.

Data may be shared for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In this case, efforts will be made to ensure the minimum data required is shared and if possible, anonymised prior to sharing.

PHOTOGRAPHY AND VIDEOS

Photographs and videos will be used where they are deemed essential for performing the public task of the school or relative to providing education. Where photographs are required for other purposes, these purposes will be documented and explicit consent will be sought, as necessary.

The retention period for photographs and videos will be documented in the retention policy. At the end of the retention period, photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

Please refer to our policy on photographs and videos.

BIOMETRIC DATA

At Patcham Infant School we do not collect any biometric data.

DATA SECURITY

Taking into account the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, we will implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk.

These measures shall include as appropriate:

- Measures to ensure that the Personal Data can be accessed only by authorised personnel for the purposes agreed in the record of processing activity and outlined in the Privacy Notice
- In assessing the appropriate level of security, account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, processing, access or disclosure of personal data
- The pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regular testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data
- Measures to identify vulnerabilities with regards to the processing of personal data in systems used to provide services to the organisation.

All staff are required to sign an acceptable use agreement, which sets out a list of measures that they must adhere to.

RETENTION POLICY

We will not keep personal data longer than necessary and will maintain a retention schedule outlining the retention requirements of electronic and paper records. We will retain the minimum amount of information that we require to carry out our statutory functions and the provision of services. Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

In circumstances where a retention period of a specific document has expired, checks will be made to confirm disposal and consideration given to the method of disposal to be used based on the data to be disposed of. These checks will include:

- Have the documents been checked to ensure they are appropriate for destruction?
- Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?

- Is retention required for evidence?
- Is retention required to meet the operational needs of the service?
- Is retention required because the document or record is of historic interest, intrinsic value or required for organisational memory?

DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example we will shred paper based records and overwrite or delete electronic files. We may use a third party to safely dispose of records on the school's behalf. If we do so, we will require guarantees that they comply with data protection law.

We aim to retain redundant emails for no longer than 3 months and operate a regular deletion schedule of emails.

TRAINING

There will be training and guidance available to all staff.

New staff will receive data protection training as part of their induction and will be required to sign any relevant acceptable use policies.

Data Protection will also form part of continuing professional development.

The school will provide a Privacy Notice to its workforce and parents/carers. This Notice will contain the following information:

- The legal basis and purpose for data processing
- The retention period and who the data is shared with
- The right to request any rectifications, erasure, consent to withdraw, to complain, data portability (if applicable) and the right to know about automated decision processes
- Loss, alteration, unauthorised disclosure of, or access to personal data.

DATA BREACHES

In the case of a personal data breach, we shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office. This is unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

In order to evaluate the personal data breach we shall inform and involve the Data Protection Officer in the assessment of the breach and in the execution of the data breach procedure to contain and manage the breach.

The notification shall at least:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- Communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects
- Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay

Personal data breaches, relating to facts, effects and the remedial action taken will be logged. The log shall enable the Information Commissioner's Officer to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in the identification of new data handling process and training requirements.

Examples of data breaches

- Loss or theft of paper records or less or theft of equipment on which data is stored eg a laptop, mobile phone, tablet device or memory stick
- A letter or email containing personal and/or confidential data sent to the wrong address (including internal staff or third parties) or an email to an unauthorised group of email boxes
- Personal data disclosed orally in error in a meeting or over the phone – including phishing where information is obtained by deceiving the organisation, or where information has been disclosed without confirming the true identity of the requester
- Unauthorised access to information classified as personal or confidential eg attaching documents to an outlook diary appointment that is openly accessible
- Posting information on the worldwide web or on a computer otherwise accessible from the internet without proper information security precautions
- Sensitive information left on a photocopier or on a desk
- Unauthorised alteration or deletion of information
- Not storing personal and confidential information securely
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale

Breaches caused by IT Security Incidents

Examples:

- Unauthorised access to IT systems because of misconfigured and/or inappropriate access controls
- Hacking or phishing attacks and related suspicious activity
- Virus or malware attacks and related suspicious activity
- ICT infrastructure-generated suspicious activity
- Divulging a password to another user without authority

SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'Subject Access Request' 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 their data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for
- 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.

We are committed to:

- Ensuring that individual's rights in their own personal information can be appropriately exercised
- Providing adequate training for staff to recognise and handle data subject access requests
- Ensuring that everyone handling personal information knows where to find further guidance on individuals' rights in relation to their own personal information
- Ensuring that queries about individuals' rights to their own personal information are dealt with effectively and promptly
- Being fair and transparent in dealing with a subject access request
- Logging all subject access requests to assist the Information Commissioner's Office with any complaints related to subject access as well as identifying any issues that may assist in the identification of new data handling process and training requirements.

All staff are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the GDPR and in compliance with this policy.

All staff have a responsibility to recognise a request for information and ensure it is passed to the responsible member of staff and/or Data Protection Officer within two working days.

Dealing with a subject access request (SAR)

What must the school do?	Why?	How?
Be clear about the nature of the request and identify what information is being requested.	Being clear about the nature of the request will enable you to decide whether the request needs to be dealt with in accordance with statutory requirements, who needs to deal with the request, and/or whether this is business as usual (BAU). If needed ask the submitter of the request for clarity.	Review the request and identify: If the request is for the personal information of the requester or made by an individual on behalf of another person (e.g. on behalf of a child or an adult lacking capacity) – this is a subject access request; If the request is for non-personal information – this may be dealt with as BAU or formally under the Freedom of Information Act 2000 (the FOIA) or the Environmental Information Regulations 2004 (the EIR). NB: The request can be received in a range of different formats e.g. letter, email, a completed form, or can be made via social media (e.g. a Facebook page or Twitter account).
If the request is a SAR the request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.	The GDPR stipulates that SARs must be completed within one month of the request – but in reality, as soon as possible.	Log the SAR in the subject access request log and inform all appropriate staff required to deal with the request.
If the information requested is for non-personal information i.e. is organisational or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows: All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.	The FOIA and EIR stipulates that requests must be completed within 20 working days of the request – therefore the more swiftly request are being dealt with, the more likely The Organisation will meet its statutory deadlines. BAU requests need to be dealt with by an individual in that particular service area who can identify and locate the information requested and provide a response within a	If the request is for non-routine/FOIA/EIR information contact the responsible member of staff (usually the Headteacher) and the Data Protection Officer.

	reasonable timeframe.	
If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection Act 2018. The request can be for either hard copy or any type of electronic information including email traffic ie the time and information that an email is sent. The request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two days.	It is in the public interest that requests are identified and dealt with as quickly as possible.	Scan and email the request to the responsible member of staff (usually the Headteacher) and the Data Protection Officer as needed.

DEFINITIONS

As defined by the GDPR

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is a person 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 by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing means any operation or set of operations which is performed on personal data or on 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;

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

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;

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or

Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;

Cross-border processing means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;
- **Relevant and reasoned objection** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and

freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

- **Information society service** means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;
- **International organisation** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- **Special categories** of personal data means personal data:
    - revealing racial or ethnic origin;
    - revealing political opinions;
    - revealing religious or philosophical beliefs or trade union membership;
    - 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;
- **Data breach**: an incident or event in which personal and/or confidential data:
    - has potentially been viewed or used by an individual unauthorised to do so;
    - has had its integrity compromised;
    - is lost or is unavailable for a significant period.