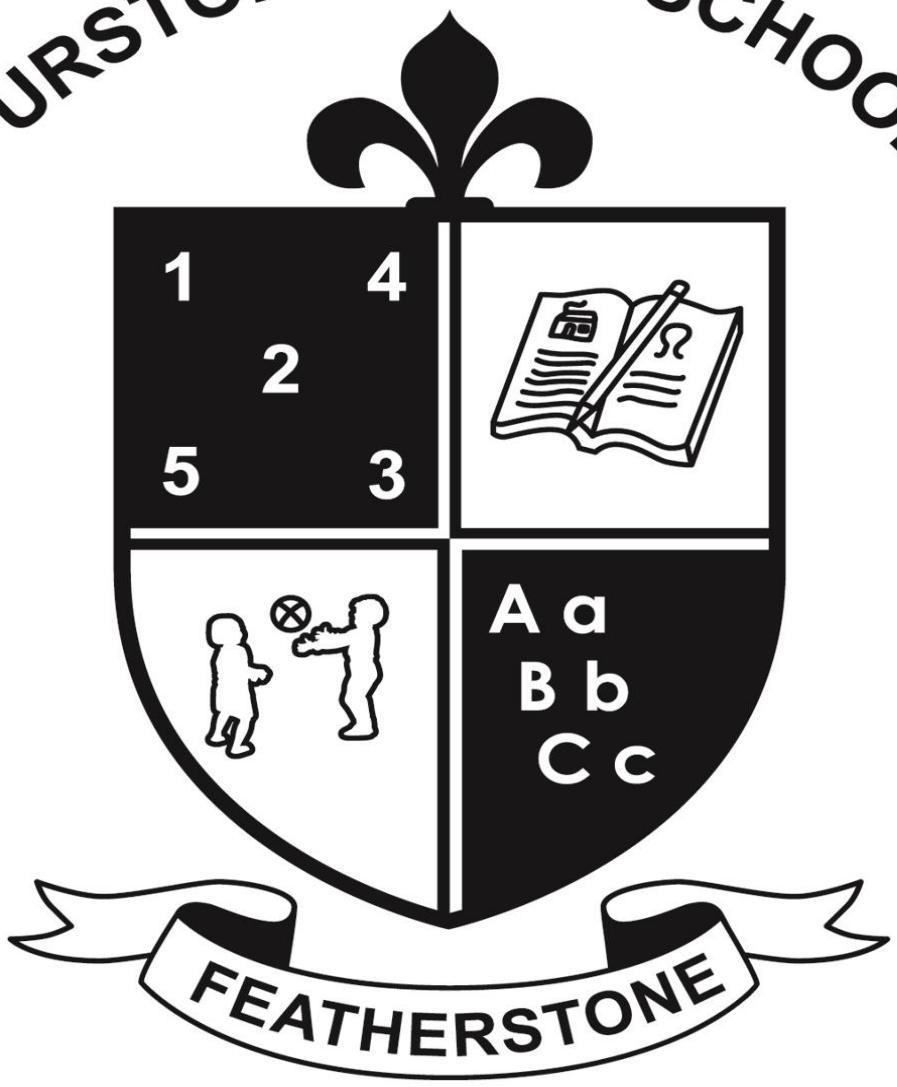
PURSTON INFANT SCHOOL



Data Protection Policy

1. Introduction

Purston Infant School aims to ensure that all personal data collected about pupils, parents, staff, governors, visitors and any other individuals is collected, stored and processed in accordance with the **General Data Protection Regulation (GDPR)** and Data Protection Act 2018 as set out in the Data Protection Bill.

This policy applies to the collection, use, storage and sharing of all personal data held by Purston Infant School in any format including paper, electronic, audio and visual.

2. Guidance

This policy complies with the requirements of the GDPR and the Data Protection Principles. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and ICO's code of practice for subject access requests (SAR). It meets the requirements of the Protection of Freedoms Act 2012 referring to any biometric data as well as the ICO's code of practice for the use of cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • 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 categories of personal 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 or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, 3 altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

We process the personal data relating to parents, pupils, staff, governors and visitors and therefore Purston Infant School is a data controller. We are registered as so with ICO and renew annually or as required. The Headteacher acts as the representative of the data controller.

5. Data protection officer

The Data protection officer (DPO) is responsible for overseeing the implementation of this policy and monitoring the schools compliance with the GDPR, other data protection laws and guidelines where applicable.

The DPO:

- Manages internal data protection activities and conducts internal data protection audits.
- Advises Governing Body on data protection assessments and issues.
- Monitors that all staff receive appropriate data protection training.
- Is the first point of contact for individuals whose data is processed (employees, parents etc) and for the ICO.

Our DPO is Mrs A Gascoyne, Deputy Headteacher, Purston Infant School, Nunns Lane, Featherstone WF7 5HF. Email : dpo@purston.wakefield.sch.uk.

6. Governing Body

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

7. All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing school of any changes to their personal data.
- Contacting the DPO in the following circumstances:
  - For information regarding this policy, retaining personal data and data security.
  - If they have any concerns that this policy is not being followed.
  - If they are unsure whether or not they have a lawful basis in which to use personal data in a particular way.

- If they need to obtain consent, deal with any data protection rights queried by an individual.
- If there is a data breach.
- Whenever they are performing a new procedure that may affect the privacy rights of an individual.
- If they require help or information regarding a new engagement or have a request to share personal data with third parties.

8. Compliance with the Data Protection Principles

School must comply with the 6 Data Protection Principles.

They say that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- 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 inaccurate personal data, with regard to the purposes for which they are processed, are erased or corrected without delay.
- Kept for no longer than is necessary for the purposes for which the personal data was processed ; Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9. Lawful processing

We will ensure that the processing of personal data fulfils the appropriate general conditions outlined in GDPR (Article 6-Lawfulness of processing)

Where Special Category Data is processed we will ensure that one of the additional conditions set out in the GDPR is also met. (Article 9 – Processing of special categories of personal data)

As a school we will only process data where we have a lawful basis to do so under data protection law:

- The data is required to fulfil a contract with the individual.
- 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 school can perform a task in the public interest, and carry out official functions.
- The data needs to be processed for the legitimate interests of the school or a third party. (provided that the individual's rights are not overridden)

- The individual, parent or carer has freely given clear consent.

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

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where a child is under 16 the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to the child.

Where consent is given, a record will be kept documenting how and when consent was given.

Consent can be withdrawn by the individual at any time.

As a Data Subject you have the following rights:

- A right of access.
- A right to rectification.
- A right to erasure in certain circumstances.
- A right to restrict processing of their personal data in certain circumstances.
- A right to data portability in certain circumstances.
- A right to object to profiling, direct marketing and/or automated decision making where applicable.

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

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 school's Data Retention Policy.

10. Sharing personal data

We will not normally share personal data with anyone else, but may do so where inter-agency working and delivery of services by a third party takes place. This could be:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers need data to enable us to provide services to our staff and pupils, e.g IT contractors. We only appoint suppliers who provide guarantees that they comply with data protection law. We will have a data sharing agreement and only share data that the supplier needs to carry out their service.

We will share personal data with law enforcement and government bodies where we are legally required to do so. This includes for:

- The prevention or detection of crime and /or fraud.

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

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

11. Right of access

Individuals have the right to obtain confirmation that their data is being processed. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Subject access requests must be submitted in writing, either by letter to school or by email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

School will then verify the identity of the person making the request before supplying information. We may ask for 2 forms of identification if clarification cannot be made via a phone call. The information will be provided free of charge; however school may impose a reasonable administration fee if further copies are requested.

All requests will be responded to without delay and at the latest within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this and will receive an explanation of why the extension is necessary.

We will not disclose 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 a child

Where a request is excessive or unfounded school reserves the right to refuse to act on it, or charge a reasonable fee which takes into account administrative costs. It will be deemed excessive or unfounded if it is repetitive, or asks for further copies of the same information.

When we refuse a request, the individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO within one month of the refusal.

12. Right of rectification, erasure and to restrict processing

In addition to access rights, individuals also have the right to:

- Withdraw their consent to processing at any time

- Ask school to rectify, erase or restrict processing of their personal data
- Object to the processing of their data when there is no overriding legitimate interest for continuing the processing
- Challenge processing which has been justified on the basis of public interest
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Requests for rectification will be responded to within one month, this will be extended to two months if complex. Where this may have been disclosed to a third party, the school will inform them where possible. Where appropriate, school will inform the individual about the disclosure. The individuals have a right to complain to the ICO if no action has been taken in response to a request.
Individuals hold the right to request deletion or removal of personal data where there is no compelling reason for its continued processing.

School has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

Individuals have the right to block or suppress the school's processing of personal data. In this event, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until school have verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

The school's data retention policy states the timeframes where various elements of data are allowed to be kept. Personal data that is no longer needed will be disposed of securely. Electronic disposal will consist of information being deleted or overwritten. Paper-based records will be shredded. We may at times ask a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that they comply with the data protection law.

13. Photographs and videos

As part of school activities, we may take photographs and record images of individuals within our setting. Uses may include:

- Inside school on notice boards, newsletters and brochures
- Outside school by external agencies such as newspapers, school photographer
- Online, through our school website, social media and apps such as Dojo

We obtain consent from parents/carers for photographs and videos as well as other communication materials before a child starts school and this remains in place until the child leaves. However consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph/video and not distribute it further. Parents/carers will be told when outside agencies are coming into school and additional consent will be sought for those activities. Children's names will not be included in any images or published on our website or newsletters.

School use Class Dojo app to message parents/carers and send images of their child and his/her class group. Any children without parent/carer permission will have their faces blocked out or if parents prefer not included in any imagery at all.

Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the Designated Safeguarding Lead believe that taking photographs or videos of any pupils would put their security at further risk, greater care will be taken towards protecting their identity.

Class Teachers are made aware of all children for whom consent was not given.

Where a parent/carer wishes to add or remove consent at any time, they should contact the school office or email the Headteacher. Written permission will be required in either circumstance on each individual child's record.

14. Confidentiality and security

All personal data will be protected and kept safe from unauthorised or unlawful access, interference, copying, processing or disclosure and from accidental or unlawful destruction, damage or loss unless permitted otherwise under the Data Protection Legislation.

Record security

- Confidential paper records are not left out on desks, pinned to notice boards/displays or left anywhere where there is general access. They are kept in a locked filing cabinet, drawer and have restricted access when not in use.
- Portable electronic devices, such as laptops, hard drives and memory sticks are kept under lock and key when not in use and will be password protected or encrypted.
- Digital data is coded, encrypted or password protected both on local and network drives. This is also backed up overnight.
- Where personal information needs to be taken off site, either in paper or electronic format, staff will take care to follow same security procedures, eg keep devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of data.
- Emails containing sensitive or confidential information are password protected or encrypted or where possible the use of Cryptshare to transfer information is preferred.

- All necessary members of staff are provided with their own secure login and password. Passwords must be minimum of 8 characters long containing numbers and letters and they will have prompts to change these regularly.
- Staff and governors will not use their own personal laptops or computers for school purposes. If using their own phones to take images, school trips etc, they must follow the same security procedures and they must download the images to a secure location and deleted from history upon return to school. They will take full responsibility for the security of the data until then.
- Visitors under no circumstances are not permitted access to personal or confidential information. Visitors to areas of school containing sensitive information are supervised at all times.

15. Data breaches

School will strive to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, school will follow the ICO guidance. The DPO will:

- Investigate and determine whether a breach has occurred. The DPO will consider whether it is accidental or unlawful. We have a duty to report certain personal data breaches.
- Keep all records of any personal data breaches regardless of whether we are required to notify ICO.
- Alert the Headteacher and Chair of Governors.
- Consider whether the breach is likely to result in a risk to people's rights and freedoms, eg. Discrimination, damage to reputation, loss of confidentiality. If so they will notify the ICO within 72 hours.
- Notify any individual affected without undue delay if it is determined to be a 'high risk' breach adversely affecting individuals' rights and freedoms.
- Complete and return all documentation required by the ICO
- Review incident, procedures involved and implement measures to stop any reoccurrence.

Updated June21