Pillarwood Farm
Pre-School

Data Protection Policy

Linked to the General Data Protection Regulation (GDPR)

May 2018

Reviewed annually

Next review May 2022

Pillarwood Farm Pre-School

Data Protection Policy

Linked to the GDPR

Created: May 2018

Review: May 2022

Statement of Intent

Pillarwood Farm Pre-School and Children's Woodland Adventures is required to keep and process certain information about its staff, setting children and school children in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The company may from time to time be required to share personal information about its staff, children and schools using our service with other organisations, mainly the LA, Department of Education, other schools and educational bodies, children's services and other third parties, such as payroll providers.

This policy is in place to ensure all staff are aware of their responsibilities and outlines how the company complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Pillarwood Farm Pre-School and Children's Woodland Adventures believes that it is good practice to keep clear policies backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25th May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

This policy will be implemented in conjunction with the following other company policies.

Legal Framework

This policy has due regard to legislation including but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- EYFS

Applicable Data

For this policy, personal data refers to information that relates to an identifiable, living individual, including information such as online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. Key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are of genetic data, biometric data and data concerning health matters.

Principles

In accordance with the requirements outlined in the GDPR, personal data will 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not 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 are inaccurate, having regard to the purposes for which they are processed, and 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 are processed; personal data may be stored for longer periods as long 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.

- The GDPR also requires that 'the controller shall be responsible for, and able to demonstrate, compliance with the principles.

Accountability

Pillarwood Farm Pre-School and Children's Woodland Adventures will implement appropriate technical and organisational measures to demonstrate data is processed in line with the principles set out in the GDPR**.**

The company will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Description of technical and organisational security measures
- Details of transfers to third countries where applicable, including documentation of the transfer mechanism safeguards in place

The setting will implement measures that meet the principles of data protection by design and data protection by default, such as,

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

Data Protection Officer (DPO)

A DPO will be appointed to:

- Inform and advise the setting and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor's the settings compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Existing employee can be appointed to the role of DPO provided that their duties are compatible with duties of DPO and do not lead to a conflict of interests. Where possible, this role will be carried out by an external provider.

The individual appointed as DPO will have professional experience and knowledge of data protection particularly that in relation to early years.

The DPO will report to the highest level of management at the setting, which is the owner.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions.

- The consent of the data subject has been obtained
- Processing is necessary for:

Compliance with a legal obligation.

The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

For the performance of a contract with the data subject or to take steps to enter into a contract.

Protecting the vital interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights of freedoms of the data subject. (This condition is not available to processing undertaken by the setting in the performance of its tasks.)

Sensitive data will only be processed under the following conditions.

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State Law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State Law which is proportionate to the aim pursued and which contains appropriate safeguards.

- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State Law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medical products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individuals wishes.
- Where consent is given a record will be kept documentation how and when consent was given.
- The school ensures that consent mechanisms meet the standards of GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- Where a child is under the age of 16 or younger if the law provides it (up to the age of 13), 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 a child.

The Right to be Informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the setting will ensure that the privacy notice is written in a plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries if applicable and the safeguards in place.

- The retention period or criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:

Withdraw consent at anytime

Lodge a complaint with a supervisory authority.

- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where the data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources will be provided.

For data obtained directly from the data subject, this information will be supplied

Within one month of having obtained the data

If disclosure to another recipient is envisaged at the latest before the data is disclosed.

If the data is used to communicate with the individual, at the latest, when the first communications takes place.

The 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.

The setting will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge, however the setting may impose a reasonable fee to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or reptatitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

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

extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the setting holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in questions has been disclosed to third parties, the setting will inform them of the rectification where possible.

Where appropriate, the setting will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within a month, this will be extended by two months if the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the setting will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority or judicial remedy.

The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws their consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data is required to be erased to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

The setting has the right to refuse a request for erasure where the personal data is being processed for 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.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing it at a later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties they will be informed about the erasure of personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment the setting will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The Right to Restrict Processing

Individuals have the right to block or suppress the setting's processing of personal data.

If processing is restricted the setting 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 the future.

The setting will restrict the processing of personal data in the following circumstances:

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

If the personal data in question has been disclosed to third parties the setting will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The setting will inform individuals when a restriction on processing has been lifted.

The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied, or transferred form one IT environment to another in a secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individuals consent or for the performance of a contract.
- When processing is cried out by automated means

Personal data will be provided in a structured commonly used and machine-readable form.

The setting will provide the information free of charge.

Where feasible, data will; be transmitted directly to another organisation at the request of the individual.

The setting is not required to adopt or maintain processing systems which are technically compatible to other organisations.

If the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The setting will respond to any requests for portability within one month.

Where the request is complex, or several requests have been received, the time frame can be extended to two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the request.

Where no action is being taken in response to a request, the setting will, without delay and at the latest within one month of the request.

Where no action is being taken in response to a request, the setting will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Object

The setting will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her situation.
- The setting will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the setting can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The setting will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The setting cannot refuse an individuals objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their situation to exercise their right to object.

Where the processing of personal data is necessary for the performance of a public interest task, the setting is not required to comply with an objection to the processing of the data.

The processing activity is outlined above, but is carried out online, the setting will offer a method for individuals to object online.

Automated Decision Making and Profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The setting will take steps to ensure that individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the setting will ensure appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The setting has the explicit consent of the individual
- The processing is necessary for reasons of substantial public interest on the basis of union/member of State Law.

Privacy by Design and Privacy Impact Assessments

The setting will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the settings data protection obligations and meeting individual's expectations of privacy.

DPIAs will allow the setting to identify and resolve problems at an early stage thus reducing associated costs and preventing damage from being caused to the settings reputation which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

DPIA will be used for more than one project, where necessary

High risk processing includes. But is not limited to, the following:

- Systematic and extensive processing activities, such a profiling.
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.
- The use of CCTV.

The setting will ensure that al DPIAs include the following information

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals.
- The measures implemented to address risk

Where a DPIA indicates high risk data processing, the setting will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Data Breaches

The term personal data breach refers to a breach of security which has led to the destruction, loss, alteration unauthorised disclosure of, or access to, personal data.

The owner will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Staff must report any data breach or potential breach as soon as possible to the data protection officer or senior member of the team.

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the setting becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case by case basis.

If a breach is likely to result in a high risk to the rights and freedoms of an individual, the setting will notify those concerned directly.

A high-risk breach means that the threshold for notifying the individual is higher that that for notifying the relevant supervisory authority.

If a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place in the setting, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate a description of the measures taken to mitigate any possible adverse effects.

Failure to report a breach when required to do so mat result in a fine, as well as a fine for the breach.

Data Security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data both on a local hard drive is password protected.

Staff are not permitted to use removable storage e.g. external hard drives or memory sticks to store data.

All electronic devices are password protected to protect the information on the device in case of theft. Devices when not in use are locked securely in a locked cabinet.

Devices holding pupil and staff photos will be regularly wiped to delete all images. Memory cards will be kept in a locked filing cabinet when not in use and wiped regularly.

Staff will not use their personal laptops or computers for the settings purpose.

Staff must not use personal email addresses for sharing and viewing any school data.

Emails containing sensitive or confidential information are password protected.

No personal data or sensitive personal data must be shared by text or on social media.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format staff will take extra care to follow the same procedure, e.g. keeping the information in a locked area.

Before sharing data, all staff members will ensure:

They are allowed to share it

That adequate security is in place to protect it.

The person or organisation who will receive the data has been outlined in a privacy notice.

The person or organisation who will receive the data have confirmed in writing that they comply with the GDPR and any other relevant data protection legislation.

Under no circumstances are volunteers, visitors, or unauthorised third parties allowed access to confidential, personal information. Those visiting areas of the setting containing sensitive information are supervised always.

Pillarwood Farm Pre-School and Children's Woodland Adventures takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

Publication of Information

Pillarwood Farm Pre-School and Children's Woodland Adventures **has information that will be routinely available including**

- **Policies and Procedures**
- **Minutes of Meetings**

Pillarwood Farm Pre-School and Children's Woodland Adventures will not publish any personal information, including photos, on its website without written permission of the individual.

Photography

The setting understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

The setting will always indicate its intentions for taking photographs of pupils and will obtain permission before using them.

If the setting wishes to use images of pupils in a publication, such as school website, prospectus, written permission will be sought for the particular usage from the parent.

Data Retention and Storing Pupil Data

Data will not be kept for longer than is necessary. The setting follows the Information Commissioner's Guidance for the retention of documents, including the Information and records Management Society's Retention Guidelines.

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.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS Data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation., as well as their responsibilities as a data handler.

Data Protection Impact Assessment

Introduction

- Project Name
- Explain what the project aims to achieve and what benefits will be to the setting, individuals and to other members of the community
- Link to any other relevant documents related to the project, e.g. a project proposal
- Describe the process for the collection and deletion of any personal data
- Explain what information will be used, what it is used for and who will have access to it
- Detail how many individuals are likely to be affected by the project

Question	Yes	No	Unsure	Comments
Will the project involve collecting new information about individuals?				
Will the project require individuals to provide information about themselves?				
Will information about individuals or organisations who have not previously held information about the individual?				
Is any information about individuals held for purposes it is not currently used for, or in a way it is not currently used?				
Will the project involve using a new technology that might be perceived as being intrusive to an individual's privacy?				
Will the project result in any decisions or actions taken against individuals which may have a significant impact on them?				
Will any information about individuals raise privacy concerns, e.g. information they may wish to keep private, such as criminal information held on DBS certificates?				
Will the project require you to contact individuals in ways that they may find intrusive?				

Risk Assessment

Potential Risk	Risk rate H/M/L	Proposed Solutions	Responsibility	Risk reduced to acceptable level Y/N
Risk to Individuals				
Risk to setting				
Risk to compliance with GDPR