Jack and Jill Pre-school

General Data Protection Regulation (GDPR) Policy

Data Protection Policy

AIM:

Our aim is to ensure that all personal data collected about staff, pupils, parents, trustees, visitors, and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to personal data whether it is in paper or electronic format.

DEFINITIONS:

|  |  |
| --- | --- |
| 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 include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.  Personal data which is equally sensitive may need more protection, including information about an individual’s:   * Racial or ethnic group * Political opinions * Religious or philosophical beliefs * Trade union membership * Genetics * Health – physical or mental * Sexual orientation |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.  Processing can be automated or manual |
| Data Subject | The identified or identifiable individual whose personal data is held or processed |
| Data Controller | A person or organisation that determines the purpose and means of processing personal data |
| Data Processor | A person or 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 |

THE DATA CONTROLLER:

Jack and Jill processes personal data relating to parents, pupils, staff, trustees, visitors, and others. It is therefore a data controller. Jack and Jill is registered with the ICO and renews its registration annually or as otherwise legally required.

ROLES AND RESPONSIBILITIES:

This policy applies to all staff employed by Jack and Jill and extends to organisations and individuals working its behalf. Staff who do not comply with this policy may face disciplinary action.

Jack and Jill’s Trustees – have overall responsibility for ensuring the relevant data protection obligations are complied with.

The Data Protection Officer (DPO) – is responsible for overseeing the implementation of this policy, monitoring our compliance with the data protection law, and developing related policies and guidelines where applicable. The DPO is the first point of contact for individuals whose data the Jack and Jill process and the ICO.

Our DPO is : Diane Shanley and is contactable via email at – [jack.jillps@hotmail.co.uk](mailto:jack.jillps@hotmail.co.uk)

All staff – are responsible for:

* Collecting, storing, and processing any personal data in accordance with this policy
* Informing Jack and Jill of any changes to their personal data, such as change of address
* Contacting the DPO in the following circumstances:
  + - * With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
      * If they have any concerns that this policy is not being followed
      * If they are unsure whether 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, or deal with data protection rights invoked by an individual.
      * If there has been a data breach
      * Whenever they are engaging in a new activity that may effect the privacy rights of individuals
      * If they need help with any contracts or sharing personal data with third parties.

DATA PROTECTION PRINCIPLES:

The GDPR is based on data protection principles that Jack and Jill must comply with. The principles say that personal data must be:

* + Processed lawfully, fairly and in a transparent manner
  + Collected for specified, explicit and legitimate purposes
  + Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
  + Accurate and, where necessary, kept up to date
  + Kept for no longer than is necessary for the purposes for which it is processed
  + Processed in a way that ensures it is appropriately secure

This policy sets out how Jack and Jill aim to comply with these principles

COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

We will only process personal data where we have on of 6 ’lawful bases’ to do so under data protection law:

1. The data needs to be processed so that Jack and Jill can fulfil a contract with individuals, or the individual has asked Jack and Jill to take specific steps before entering into a contract
2. The data needs to be processed so that Jack and Jill can comply with legal obligation
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life
4. The data needs to be processed so that Jack and Jill can perform a task in the public interest, and carry out its official functions
5. The data needs to be processed for the legitimate interests of Jack and Jill or a third party (provided the individual’s rights and freedoms are not overridden)
6. The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent.

Limitation, minimisation and accuracy

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 the 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 Jack and Jill’s retention schedule.

SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

* There is an issue with a child 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 or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this we will only appoint suppliers and contractors which can provide sufficient guarantees that they comply with data protection law and only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

* The prevention or detection of crime and / or fraud
* The apprehension or prosecution of offenders
* The assessment or collection of tax owed to HMRC
* In connection with legal proceedings
* Where the disclosure is required to satisfy our safeguarding obligations

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.

SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS:

Subject Access Requests:

Individuals have a right to make a subject access request to gain access to personal information that Jack and Jill holds about them. This includes:

* Confirmation that their personal data is being processed
* Access to a copy of the data
* The categories of personal data concerned
* Who the data has been or will be shared with
* How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
* The source of the data, if not the individual
* Whether any automated decision-making is being applied to their data, and what the significance and consequence of this might be for the individual

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

* Name of the individual
* Correspondence address
* Correct number and email address
* Details of the information requested

If staff receive a subject data access request they must immediately forward it to the DPO

Children and subject access requests:

Personal data about children belongs to that child, and not the child’s parent or carer. For a parent or carer to make a subject access request with respect to their child , the child must be either able to understand their rights and the implications of a subject access request, or have given their written consent. Children below the age of 12 are not generally regarded to be mature enough to understand their rights and the implications of subject access requests. Therefore, subject access requests from parents or carers of children at Jack and Jill may be granted without the express permission of the pupil. This is not a rule and pupils ability to understand their rights will always be judged on a case-by-case basis

Responding to Subject access requests:

When responding to requests we –

* May ask individuals to provide two forms of identification
* May contact the individual via phone to confirm that the request was made
* Will respond without delay and within one month of receipt of the request
* Will provide the information free of charge
* May tell the individual we will comly within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary. We will not disclose information if it:
  + Might cause serious harm to the physical or mental health of a pupil or another individual
  + Would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child’s best interests
  + Is contained in adoption or parental order records
  + Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

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

The data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have a right to:

* Withdraw their consent to processing at any time
* Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it.
* Prevent use of their personal data for direct marketing
* Challenging processing which has been justified based on public interest
* Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
* 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 the personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO

PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents, or those with parental responsibility, have a legal right to free access to their child’s educational record. This can be accessed via Parent Zone at any time, other records will be supplied within 15 days of receipt of a written request.

PHOTOGRAPHS AND VIDEOS

As part of Jack and Jill’s activities, we make take photographs and record images og individual within the settings. We will obtain written consent form parents/carers for these to be taken of their child for communication, marketing, and promotional materials. We will clearly explain how the photographs or video will be used to both the parent/carer and child.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photographs or videos and not distribute them further. When using photographs and videos in this way we will not add any other personal information about the child, to ensure they cannot be identified.

DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

* Appointing an appropriate DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their knowledge
* Only processing data that is necessary for specific purpose of processing, and always in line with the data protection principles
* Integrating data protection into internal documents
* Regularly training members on data protection law, this policy and related policies

DATA SECURITY AND SECURITY STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

* Paper-based records and portable electronic devices that contain personal data are kept securely when not in use
* Papers containing confidential personal data must not be left on office or ‘classroom’ desks, staff room tables, pinned to noticeboards or left anywhere else where there is general access
* Where personal information needs to be taken off site it must be securely stored and returned as soon as possible
* Passwords are used to access Jack and Jill’s computers, laptops, staff accounts and other electronic devices
* Staff, children or trustees who store personal information on their personal devices are expected to follow the same security procedures as for Jack and Jill owned equipment
* Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.
* Where using a virtual personal assistant to access music and stories we will use the built-in privacy protection methods, such as microphone off buttons, camera covers, light indicators and no recording settings to ensure that sensitive data is not recorded and stored. Regular checks will be completed to ensure the device settings remain compliant with this policy.

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 or incinerate paper-based records, and overwrite or delete electronic files.

PERSONAL DATA BREACHES

Jack and Jill will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow a set procedure and make a report to the ICO within 72 hours.

TRAINING

All staff and trustees are provided with data protection training as part of their induction process or as soon as practically possible. Data protection will form part of Jack and Jill’s CPD programme

This policy was adopted by Jack and Jill Pre-school at a meeting held on: 13th October 2022

It is signed on behalf of the setting by: Lynne Batchelor, Chairperson