



DATA PROTECTION AND PRIVACY POLICY

FOR EMPLOYEES; CHILDREN ATTENDING KIDS PLANET

NURSERIES; THEIR PARENTS AND KIDS PLANET VISITORS



Contents

- THE PURPOSE OF THIS DOCUMENT** 4
- LEGISLATION**..... 4
- DATA PROTECTION PRINCIPLES** 4
- THE KIND OF INFORMATION WE HOLD ABOUT YOU**..... 5
 - Employees* 5
 - Children* 6
 - Parents* 7
 - Frequently Queried Processing Activities* 7
 - Website** 7
 - Biometrics** 7
 - CCTV:** 8
- HOW YOUR PERSONAL INFORMATION IS COLLECTED** 9
 - Employees* 9
 - Children and Parents* 9
- HOW WE WILL USE INFORMATION ABOUT YOU** 9
 - SITUATIONS IN WHICH WE WILL USE EMPLOYEE PERSONAL INFORMATION* 9
 - SITUATIONS IN WHICH THE NURSERY WILL USE PERSONAL INFORMATION OF CHILDREN* 10
 - SITUATIONS IN WHICH THE NURSERY WILL USE PERSONAL INFORMATION OF PARENTS*..... 11
 - IF EMPLOYEES AND PARENTS FAIL TO PROVIDE PERSONAL INFORMATION* 11
 - CHANGE OF PURPOSE* 11
 - HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION* 11
- THE NURSERY’S OBLIGATIONS AS AN EMPLOYER** 12
 - FURTHER MEASURES FOR ENSURING CONFIDENTIALITY* 12
 - DO WE NEED EMPLOYEE CONSENT?* 13
 - INFORMATION ABOUT CRIMINAL CONVICTIONS* 13
 - AUTOMATED DECISION-MAKING*..... 13
- DATA SHARING** 14
 - WHY MIGHT THE NURSERY SHARE EMPLOYEE, CHILD OR PARENT PERSONAL INFORMATION WITH THIRD PARTIES?* .. 14
 - THIRD-PARTY SERVICE PROVIDERS* 14
 - WHAT ABOUT OTHER THIRD PARTIES?*..... 14
 - DATA RETENTION*..... 14
- RIGHTS AND DUTIES** 15
 - Your duty to inform us of changes* 15



Your rights in connection with personal information..... 15

RIGHT TO WITHDRAW CONSENT 16

RESOURCES 16

Data Protection Officer 16

CHANGES TO THIS POLICY AND PRIVACY NOTICE 16

APPENDIX 1: Procedure for Reporting a Breach 17

APPENDIX 2: Subject Access Request Procedure 19

If you have any questions about this policy, please contact Karen Seddon:
Karen.seddon@kidsplanetdaynurseries.co.uk

THE PURPOSE OF THIS DOCUMENT

Kids Planet (“the Nursery” or “we”) is committed to protecting the privacy and security of your personal information. This privacy notice describes how the Nursery collects and uses personal information about employees of the Nursery (“Employees”), children attending the Nursery (“Child” or “Children”) and the parents of the Children (“Parents”) (known collectively as “You” or “Your”), in accordance with the General Data Protection Regulations (GDPR).

As part of the Kids Planet group, Kids Planet is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about You. We are required under data protection legislation to notify You of the information contained in this privacy notice.

This notice applies to Employees, Children and Parents, as well as visitors to Kids Planet. This notice does not form part of any contract of employment or other contract to provide services.

It is especially important that Employees and Parents read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about You, so that You are aware of how and why we are using such information and what Your rights are under the data protection legislation.

Employees, Parents and visitors can access this document on the Kids Planet website and can request a copy at any time from a Kids Planet reception desk or from our Central Support office.

LEGISLATION

- We follow the legal requirements set out in the Statutory Framework for the Early Years Foundation Stage (EYFS) 2017 and accompanying regulations about the information we must hold about registered children and their families and the staff working at the nursery.
- We follow the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 with regard to the storage of data and access to it.
- Kids Planet Day Nurseries Ltd is registered with the ICO, reference Z2484469, as a tier 3 data controller.

DATA PROTECTION PRINCIPLES

Kids Planet are compliant with data protection legislation as it applies in the UK. There are seven key principles outlined in the legislation and with which we adhere:

1. *Lawfulness, fairness and transparency*
2. *Purpose limitation*: we process personal data only for valid purposes that we have clearly explained to You and not used in any way that is incompatible with those purposes).
3. *Data minimisation*: we process data that is relevant to the purposes we have told You about and limit processing only to those purposes.
4. *Accuracy*: we do all we reasonably can to ensure the personal data we hold, is accurate and up to date.
5. *Storage limitation*: We retain personal data only as long as necessary for the purposes we have told You about.
6. *Integrity and confidentiality*: we do all we reasonably can to ensure personal data is held securely.
7. *Accountability*: we accept responsibility as a data controller to demonstrate compliance with data protection legislation.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

Details of the data processed by Kids Planet, includes:

- 🔍 Personal data – data that personally identifies you, such as name and contact details
- 🔍 Special Category data – data that may reveal a characteristic of identity, such as race or sexual orientation or your health. Examples include passports and health declarations.
- 🔍 Criminal Offence Data, such as references to DBS certificates and self-disclosure.

Employees

We may collect, store, and use the following categories of personal information about Employees:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Copies of identification documents, such as passport and utility bill
- Next of kin and emergency contact information.
- National Insurance number.
- Photographs e.g. Selima profile; About Me photo and photos of activities in the rooms
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of an Employee’s continuous employment.
- Location of employment or workplace.
- Driving licence (where applicable) information.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- DBS self-declaration and details from the enhanced DBS with children’s barred list checks
- Disciplinary information and investigations; safeguarding allegations or issues; appraisals and reviews.
- Details of company pension, pay, bonus, expenses and benefits, such as UK Healthcare; pay day advances and all deductions.
- Personnel files and training records including performance information, disciplinary and grievance information, and working time records.
- Information about your use of our information and communications systems.
- Records of any reportable death, injury, disease or dangerous occurrence.

- Information about an Employee's race or ethnicity.
- Your signature e.g. when signing forms and contracts
- Information about an Employee's health, including any medical condition, accident, health and sickness records, including:
 - where an Employee leaves employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
 - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave including Bradford scores; and
 - where an Employee leaves employment and the reason for leaving is related to their health, information about that condition needed for pensions and permanent health insurance purposes.

Children

Kids Planet give particular weight to the rights and interests of children. This means, on the one hand, that we are especially concerned with the protection of children's data. On the other hand, it means that our duty to safeguard the health and well-being of children is paramount and takes precedence over our duties under the GDPR. For example, paragraph 62 of Keeping Children Safe in Education affirms that while data protection legislation "...places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information, where the failure to do so would result in a child being placed at risk of harm. Fears about sharing information cannot be allowed to stand in the way of the need to promote the welfare and protect the safety of children."

We may collect, store, and use the following categories of personal information about Children:

- Name
- Date of birth
- Home address
- Dietary requirements
- Attendance and absence information
- Photographs and video clips of the Child to signpost Children to where their belongings are stored at the Nursery that they attend, and also for general display purposes
- Emergency contact's contact details
- Record book for each Child containing the work of the Child while at the Nursery, observations about the Child's development while at the Nursery from Employees of the Nursery, specific examples of the Child's progress, photographs demonstrating the Child's development whilst at the Nursery, and personal details of the Child (e.g. their date of birth) ("Progress Report")
- Information relating to any special educational needs or disabilities
- Records relating to individual Children e.g. care plans, common assessment frameworks, speech and language referral forms
- Accidents and pre-existing injuries forms
- Records of any reportable death, injury, disease or dangerous occurrence
- Observation, planning and assessment records of Children
- Records of any safeguarding concerns or allegations
- Information about a Child's race or ethnicity, spoken language and nationality.
- Information about a Child's health, including any medical condition, health and sickness records.
- Information about a Child's accident or incident reports including reports of pre-existing injuries.
- Information about a Child's incident forms / child protection referral forms / child protection case details / reports.

Parents

We will collect, store, and use the following categories of personal information about Parents:

- Name
- Contact details including home address, telephone numbers, email addresses.
- National Insurance number.
- Bank account details.
- Your signature e.g. on contracts and consent forms
- Information about a Parent's race or ethnicity, spoken language and nationality.
- Conversations with Parents where Employees of the Nursery deem it relevant to the prevention of radicalisation or other aspects of the governments Prevent strategy.
- Conversations with parents about safeguarding concerns or allegations.

Frequently Queried Processing Activities

Website:

- IP addresses may be tracked along their journey through our website, in order for us to analyse customer needs and continually improve our service.
- Cookies provide information about the computer used by a website visitor and they are downloaded onto the visitors hard drive. Cookie notices are enabled on the website. You can reject cookies, by altering the cookie settings on your computer.
- The information we collect using cookies, does not identify you personally. Your identity is revealed to us when you identify yourself, such as by filling out a website form. Once you identify yourself, we can then match your identity to your journey through our website.
- Your information is not sold to third parties.
- Once we know who you are, we may contact you to ask whether you would like to receive promotional messages, such as details of new services on offer; Kids Planet competitions and offers of promotional fees. If you consent to receiving these communications, you can withdraw your consent at any time by contacting Central Support.
- The sending of information via the internet is never totally secure and on occasion, can be unlawfully intercepted. We therefore cannot guarantee the safety of your electronic data, but we can reassure you that Kids Planet take all reasonable steps to ensure the information you provide to us is held securely and that our data processing is lawful and responsible.
- We occasionally include links to third parties on our website (e.g. Money Saving Expert for a simple guide to childcare funding). Where we provide a link, this does not mean that we endorse or approve that site's policy towards visitor privacy. You should review their privacy policy before sending them any personal data.

Biometrics:

- Biometric data, when used in order to identify a person, is Special Category data, under GDPR.
- We use systems for individual biometric access.
- The reader takes reference points from the finger, in order to create an algorithm (numbers not images) that can be matched against a person who is authorised to access the area.
- The algorithm cannot be converted into a fingerprint or image. It cannot be used to gain access to any other device.

- Algorithms are stored within the hard drive of the control unit on site. There is no cloud storage and no remote access to this data.
- The risk of any impact upon your privacy, is very low.
- We rely upon our legitimate interest in the safety and security of our facilities / facility users, as our lawful basis for processing biometric data. This legitimate interest is also cited in our data audit as the special condition required for processing biometric information.
- This means that if a colleague or parent objects to Kids Planet processing their biometric data, their particular situation will be balanced against our legitimate interests in safety and security.

CCTV:

- Kids Planet has in place a CCTV surveillance system, comprising of fixed position cameras; pan, tilt and zoom cameras; monitors; multiplexers; digital recorders and public information signs..
- Cameras are placed strategically, to cover communal areas, such as reception and team room. In some nurseries, there are cameras in the children's rooms, gardens and carpark. Cameras are not hidden from view.
- Each recorder contains a hard drive on which images are stored 24 hours per day in real time mode. Images are overridden as further images are stored so, depending on memory of the individual recording unit, images are typically overridden every 2 to 3 weeks.
- Monitors are not visible from outside the premises and are monitored by colleagues who are authorised to do so, in accordance with the purposes of the system as outlined below.
- There are clear signs placed in prominent places, to inform all users of the premises that CCTV is in operation.
- Nursery / Centre Managers are responsible for the operation of the system and ensuring strict compliance with this policy.
- The lawful basis for processing CCTV data, is our legitimate interest in the safety and security of persons and property as well as safeguarding children. The images can also help to resolve disputable incidents. These purposes are achieved by monitoring CCTV images in order to:
 - Ensure children are appropriately cared for
 - Assist in the prevention of crime
 - Provide evidence in investigations such as disciplinary investigations and safeguarding allegations
 - Provide opportunities for staff training
- Images that identify data subjects are not shared with third parties (or published on the internet / social media) without your consent, unless Kids Planet become legally obliged to share the data, by law enforcement agencies; prosecution agencies or a court of law and in some case, emergency services in connection with investigation of an incident.
- If the police request that CCTV footage is shared with them, authorisation is not required and the person in charge of the nursery, should share the requested footage straight away. The footage will be shared with police by way of a secure method agreed with them and after verifying police identity. After sharing footage with police, you must email Clare Roberts and/or a Company Director to inform them.
- Kids Planet do not share copies of CCTV footage with any parties, unless required by a law enforcement officer or a court order.
- Parents and data subjects wishing to view CCTV footage of themselves or their own children, can be given a CCTV transcript or they can arrange to come into nursery to view the footage on screen. Please liaise with your Area manager when making these arrangements and consider the impact or any potential risks to other data subjects who may be viewed on screen.
- Our special condition for processing CCTV data, is also our legitimate interest in safety and security.
- Faults or issues with equipment and lost recordings should be reported to the Area Manager and to Head Office, in a timely manner. Managers check the system daily as part of their opening checks.

HOW YOUR PERSONAL INFORMATION IS COLLECTED

Employees

We collect personal information about Employees through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of when an Employee works for us.

We collect information relating to disciplinary investigations and safeguarding allegations, from colleagues, internal registers, CCTV footage and other internal sources. In these circumstances we may also collect information from external sources, such as social services, the LADO, Ofsted and the police.

Children and Parents

We collect personal information about Children and Parents from when the initial enquiry is made by the Parents, through the enrolment process and until the Children stop using the Nursery's services.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use Your personal information when the law allows us to. Most commonly, we will use Your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with You.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and Your interests and fundamental rights do not override those interests.
4. We have obtained Your consent to process your data

We may also use Your personal information in the following situations, which are likely to be rare:

1. Where we need to protect Your vital interests (or someone else's vital interests) i.e. to protect life.
2. Where it is needed in the public interest or for official purposes.
3. For the purposes of legal claims.

SITUATIONS IN WHICH WE WILL USE EMPLOYEE PERSONAL INFORMATION

We need all the categories of information listed in this policy (see Employee section within the Paragraph entitled 'The Kind of Information We Hold About You') primarily to allow us to perform our contracts with Employees and to enable us to comply with legal obligations. The situations in which we will process Employee personal information are listed below.

- Making a decision about an Employee's recruitment or appointment.
- Checking an Employee is legally entitled to work in the UK. Paying an Employee and, if an Employee is an Employee or deemed Employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Providing any Employee benefits to Employees.
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Liaising with the trustees or managers of a pension arrangement operated by a group company, your

pension provider and any other provider of employee benefits.

- Administering the contract we have entered into with an Employee.
- Conducting performance and/or salary reviews, managing performance and determining performance requirements.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about an Employee's continued employment, engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving Employees, including accidents at work.
- Ascertaining an Employee's fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Equal opportunities monitoring.
- Safeguarding and related investigations

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of an Employee's personal information.

SITUATIONS IN WHICH THE NURSERY WILL USE PERSONAL INFORMATION OF CHILDREN

We need all the categories of information in the list above (see Children section within the Paragraph entitled 'The Kind of Information We Hold About You') primarily to allow us to perform our obligations (including our legal obligations to Children). The situations in which we will process personal information of Children are listed below.

- Upon consent from the Parents, Personal Data of Children will be shared with schools for progression into the next stage of their education.
- Personal information of Children will be shared with local authorities without the consent of Parents where there is a situation where child protection is necessary. However, where appropriate, we will consult parents when sharing information relating to safeguarding and child protection.
- The personal information of Children will be shared with local authorities with the consent of Parents for funding purposes.
- Ofsted will be allowed access to the Nursery's systems to review child protection records.
 - To ensure we meet the needs of the Children
 - To enable the appropriate funding to be received
 - Report on a Child's progress whilst with the Nursery
 - To check safeguarding records
 - To check complaint records
 - To check attendance patterns are recorded
 - When a Child's Progress Report is given to its Parent in order for that Parent to pass the same Progress Report to a school for application or enrolment purposes

SITUATIONS IN WHICH THE NURSERY WILL USE PERSONAL INFORMATION OF PARENTS

We need all the categories of information in the list above (see Parents section within the Paragraph entitled 'The Kind of Information we Hold About You') primarily to allow us to perform our contracts with Parents and to enable us to comply with legal obligations. The situations in which we will process personal information of Parents are listed below.

- The personal information of Parents will be shared with local authorities without the consent of Parents for funding purposes.
- To report on a Child's attendance
- To be able to contact a Parent or a Child's emergency contact about their Child
- To ensure nursery fees are paid

IF EMPLOYEES AND PARENTS FAIL TO PROVIDE PERSONAL INFORMATION

If Employees and Parents fail to provide certain information when requested, we may not be able to perform the respective contracts we have entered into with Employees and Parents, or we may be prevented from complying with our respective legal obligations to Employees, Children and Parents.

CHANGE OF PURPOSE

We will only use Your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use Your personal information for an unrelated purpose, we will notify the Employee, Child or Parent, as is appropriate in the circumstances, and we will explain the legal basis which allows us to do so.

Please note that we may process an Employee's, a Child's or a Parent's personal information without their respective knowledge or consent, as relevant to the circumstances, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with Employee or Parent explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with Employee employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect an Employee, a Child or a Parents' interests (or someone else's interests) and the Employee, Child or Parent as is appropriate is not capable of giving consent, or where the Employee or Parent has already made the information public.

THE NURSERY'S OBLIGATIONS AS AN EMPLOYER

We will use particularly sensitive personal information of Employees in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about the physical or mental health of an Employee, or their disability status, to ensure Employee health and safety in the workplace and to assess the fitness of Employees to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.
- We will use information about an Employee's race or national or ethnic origin, religious, philosophical or moral beliefs, or an Employee's sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

FURTHER MEASURES FOR ENSURING CONFIDENTIALITY

It is our intention to respect the privacy of children, their families and our team. Measures in place for ensuring confidentiality include:

- Storing confidential records in a locked filing cabinet.
- Ensuring the Nursery Office door is locked when unmanned.
- Keeping reception desks clear of personal data or ensuring it is hidden from view.
- Team awareness of confidentiality of personal data.
- Ensuring parents can access files and records of their own children but not those of any other child.
- Care when discussing personal information, ensuring it is discussed on a 'need to know' basis (i.e. necessary according to the processing purpose) and not overheard.
- Team abide by our social media policy and code of conduct, which warn against disclosing information about children on their own personal social media or in any way to members of the general public, including friends and family.
- Company induction includes awareness of the importance of confidentiality and data protection.
- Issues concerning the team are confidential to those directly involved with making personnel decisions.
- Any concerns/evidence relating to a child's personal safety are held securely and shared with as few people as possible on a 'need-to-know' basis. If a child is considered at risk our Safeguarding Policy will override confidentiality.
- Confidential information in Central Support / Head Office is kept behind a locked door, accessible only by persons for whom access to the office is necessary to their role.
- Electronic files are password protected. Passwords are changed regularly. File / folder permissions are limited to persons for whom access is necessary to their role.
- Team with email accounts can access Kids Planet emails on their personal devices, only with permission from the CEO.
- Team working from home can access Kids Planet systems via a VPN and dual verification software, only with permission from the CEO.

DO WE NEED EMPLOYEE CONSENT?

We do not need the consent of Employees if we use special categories of personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach Employees for their written consent to allow us to process certain particularly sensitive data. If we do so, we will provide Employees with full details of the information that we would like and the reason we need it, so that Employees can carefully consider whether they wish to consent. Employees should be aware that it is not a condition of their contract with the nursery that they agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect the interests of You (or someone else's interests) and You are not capable of giving your consent, or where an Employee or a Parent, as is relevant to the circumstances, has already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so, which includes but is not limited to Disclosure and Barring Service ("DBS") checks. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions to conduct a DBS check on each Employee, to record the date of the DBS check, the number of the DBS check and the name of the body conducting the DBS check.

We are allowed to use your personal information in this way to carry out our obligations. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified Employees or Parents of the decision and given the Employee or the Parent as is appropriate 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with an Employee or a Parent and appropriate measures are in place to safeguard the Employee's, the Child's or the Parent's rights as is appropriate.

3. In limited circumstances, with explicit written consent from the Employee or the Parent, as is appropriate, and where appropriate measures are in place to safeguard Employee or Parent rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either explicit written consent from an Employee or a Parent as is appropriate, or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard an Employee or a Parents rights as is relevant in the circumstances.

You will not be subject to decisions that will have a significant impact on You based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified the Employee or the Parent as is appropriate in the circumstances.

DATA SHARING

We may have to share Employee, Child or Parent data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of Your data and to treat it in accordance with the law.

WHY MIGHT THE NURSERY SHARE EMPLOYEE, CHILD OR PARENT PERSONAL INFORMATION WITH THIRD PARTIES?

We will share Your personal information with third parties where required by law, where it is necessary to administer the working relationship with You or where we have another legitimate interest in doing so.

THIRD-PARTY SERVICE PROVIDERS

"Third parties" includes third-party service providers (including contractors and designated agents), local authorities, regulatory bodies, schools and other entities within our group. The following third-party service providers process personal information about you for the following purposes:

- Local Authorities – for funding and monitoring reasons (e.g. equal opportunities and uptake of funded hours)
- Regulatory bodies – for ensuring compliance and the safety and welfare of the children
- Schools – to provide a successful transition by ensuring information about the child's progress and current level of development and interests are shared

We will share personal data regarding your participation in any pension arrangement operated by a group company with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

WHAT ABOUT OTHER THIRD PARTIES?

We may share Your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share Your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share Your personal information with a regulator or to otherwise comply with the law.

DATA RETENTION

Please see the *Retention and Archiving Policy* for full details. We will only retain Your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of Your personal data, the purposes for which we process Your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise Your personal information so that it can no longer be associated with You, in which case we may use such information without further notice to You. Once you are no longer an Employee, or a Child benefiting from the Nursery's services or a Parent, as is appropriate, we will retain and securely destroy your personal information in line with this policy and the Kids Planet *Retention and Archiving Policy*.

RIGHTS AND DUTIES

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

The GDPR affords 7 individual rights. Not all of the rights are absolute –there are conditions attached to some and in most cases, a balanced approach to entitlement and interests, is promoted by the regulations.

1. The right to **be informed** about the processing of your data.
Kids Planet actively inform colleagues and parents about the data we process. Our policies and procedures for processing data, are transparent, accessible and intelligible. We issue privacy notices where appropriate.
2. The right to **access** data that Kids Planet hold about you or your child
You can request to be informed about or see data we hold about you or your child or request to verify the lawful basis for our processing of your data. For the *Subject Access Request Procedure* see Appendix 2
3. The right to **rectify** data that is incorrect or incomplete
Most rectification requests can be resolved informally, by speaking with the person in charge of the information, such as a Centre Manager, Customer Support or the reception team. Occasionally, a parent or colleague may wish to make a formal rectification request. Kids Planet will consider whether the data is inaccurate and other factors, such as whether an inaccurate account (such as a false allegation) was rectified but the inaccurate account was lawfully retained. If Kids Planet shared inaccurate information with third parties, we will where possible (and not disproportionate), inform them of rectifications made.
4. The right to **erase** your data - sometimes known as ‘the right to be forgotten’.
Kids Planet will consider the relevance of the data you wish to erase and whether it is necessary for us to retain or erase the information due to an overriding obligation or legitimate interest. If Kids Planet have shared the erased information with third parties, we will where possible (and not disproportionate), inform them of the erasure.
5. The right to **restrict** processing, by insisting that data held about you is not used.
Requests for data restriction are an alternative to erasure and may be temporary, such as while the lawfulness or accuracy of data processing is being verified or in order to support a legal claim.
Procedures for restricting processing are variable, for example:
 - Removing the data from our website, but retaining within a password protected file.
 - Making an exception to auto-deletion of an ex-colleague’s file.
 - Creating a secure file for information that may be processed if and when the restriction is lifted.You will be informed before a restriction is lifted, with reasons that the restriction no longer applies. If Kids Planet have shared the restricted information with third parties, we will where possible (and not disproportionate), inform them of the restriction.
6. The right to **data portability** allows you to reuse your data to access different services.
This right applies only to personal data that you provide to Kids Planet and is processed by automated means, such as website search / usage history. If the right applies, you can request a copy of the data and / or to have the data transmitted by Kids Planet, to another controller.
7. The right to **object** to the processing of your data
This right applies only when our lawful basis for processing the data is a legitimate interest of Kids Planet; used for direct marketing or used for research / statistics. You have an absolute right to object to direct marketing. If you object to receiving promotional offers, Kids Planet will no longer send you this information, even if you previously asked to be included. In other cases, the regulations require a balanced approach, weighing your particular situation and reasons for objecting, against any compelling reasons for processing the data.



RIGHT TO WITHDRAW CONSENT

In circumstances where You may have provided Your consent to the collection, processing and transfer of Your personal information for a specific purpose, You have the right to withdraw Your consent for that specific processing at any time. To withdraw Your consent, contact the person in charge of the nursery. Once we have received notification that You have withdrawn Your consent, we will no longer process Your information for the purpose or purposes You originally agreed to, unless we have another lawful basis for doing so.

RESOURCES

Kids Planet provide colleagues with the tools they need to be responsible data processors, including:

- Secure operating systems with a GDPR compliant provider.
- Remote working safeguards, such as a secure VPN.
- Frequent password resetting requirement.
- Confidential waste facilities.
- Secure archiving facilities.
- Confidential system for visitor sign-in.

Data protection forms part of basic Kids Planet training, delivered to all colleagues, by way of induction training and the Colleague Handbook including Code of Conduct. Many aspects of GDPR compliance are captured within other training packages.

Data Protection Officer (DPO)

The company DPO is Karen Seddon:

EMAIL: karen.seddon@kidsplanetdaynurseries.co.uk

POST: 231 Higher Lane, Lymm, WA13 0RZ

CHANGES TO THIS POLICY AND PRIVACY NOTICE

We reserve the right to update this policy and privacy notice at any time, and we will provide an updated copy upon request. Alternatively, you can access this document on our website. When we make substantial changes, we will proactively notify you if necessary and no changes made to the policy and privacy notice affect your GDPR rights.

APPENDIX 1: Procedure for Reporting a Breach

All breaches of data should be reported internally to Karen Seddon, as soon as the breach is known: karen.seddon@kidsplanetdaynurseryseries.co.uk

How much time do we have to report a breach?

Notifiable breaches must be reported to the ICO without undue delay and not later than 72 hours after becoming aware of it. Reasons for any delay must be given and information can be provided in phases rather than all at once, provided this is done without undue delay. Breaches are reported by the company DPO (Karen Seddon).

How do we decide whether a breach is notifiable?

The ICO have an online self-assessment tool: <https://ico.org.uk/for-organisations/report-a-breach/>

The tool asks about whether the breach represents **ANY** risk to individuals and you may need expert assistance (for example from our IT providers) to help with answering this question.

If we are in doubt on whether a breach is notifiable, we will take legal advice.

The self-assessment and any discussion with lawyers further to the self-assessment are conducted by the company DPO (Karen Seddon).

How do we report a notifiable breach to the ICO?

The same ICO page [<https://ico.org.uk/for-organisations/report-a-breach/>] contains a link for reporting a notifiable breach if that is necessary. The online form asks for details such as the type of data breached; an account of the data breach; likely consequences and what we have done, for example to retrieve and re-secure the data. Notifiable data breaches are reported by the company DPO (Karen Seddon).

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

When do we need to tell individuals about a breach?

If a breach is likely to result in a **HIGH** risk to the rights and freedoms of individuals, you must inform those concerned directly and without undue delay.

If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Please take advice from the company DPO before deciding whether to tell individuals about a breach.

What information must we provide to individuals when telling them about a breach?

In clear and plain language, describe the nature of the data breach; a description of what happened and likely consequences, as well as measures we have taken to deal with the breach and potential adverse effects.

What should I record?

Document all data breaches, regardless of whether or not they need to be reported to the ICO. Record what happened, likely risks and consequences as well as measures taken, including the self-assessment when deciding whether to report the breach to the ICO. If appropriate, there should be an investigation and measures put in place to prevent a similar breach, such as re-training of individuals or a change in policy. Internal records will be made by the company DPO (Karen Seddon)

What else should we involve?

It may be appropriate to involve third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.



APPENDIX 2: Subject Access Request Procedure

- IF YOU RECEIVE A SUBJECT ACCESS REQUEST IN YOUR SETTING, CONTACT KAREN SEDDON FOR SUPPORT WITH THIS PROCESS.
- Many issues can be resolved at setting / department level, as they arise. Examples include amending contact details or withdrawing consent to display photographs.
- Formal requests should be made to Head Office in writing and your request will be directed to the appropriate department for the information you have requested:

<p>By Post</p> <p>Kids Planet Day Nurseries - Head Office 231 Higher Lane Lymn WA13 0RZ</p>	<p>By Telephone</p> <p>01925 753448</p> <p>By Email</p> <p>head.office@kidsplanetdaynurseries.co.uk</p>
--	---

- Kids Planet will respond to you within 1 month from the day following your request. You will receive one of three responses at this point:
 - 1) Agreement with your request and an explanation of how and when your request will be followed.
 - 2) Refusal of your request, along with details of the considerations made and how Kids Planet have justified this decision.
 - 3) Reasons why Kids Planet require more time to consider your request, such as in complex cases or cases in which we are awaiting payment of a reasonable fee.
- Please note that, when making requests under GDPR, it may be necessary for us to request further information from you, such as to verify your ownership of the data, by requesting photo ID.
- Responses will be given in a structured and commonly used format, such as a spreadsheet or pdf. If you prefer a different format or do not understand the response, please contact Central Support, who will spend time in ensuring you can access and understand the response.
- Actions and considerations based on your request are necessarily variable. If you need a deeper understanding of the factors involved, please contact Head Office or visit the ICO web page for full information on how to exercise your rights under GDPR: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>
- A charge will not be made for actions and considerations based on GDPR requests, unless the request is manifestly unfounded or unreasonably excessive / repetitive, in which case Kids Planet may charge a reasonable fee and also reserve the right not to respond to the request. If a reasonable fee is charged, you will be informed of this decision, including justification of the decision and the request will not be actioned until the fee is paid.
- If you feel your GDPR rights have not been upheld, we encourage you to talk to us and we will make all reasonable efforts to resolve the issue.
- The company contact for Data Protection matters is Karen Seddon:
Karen.seddon@kidsplanetdaynurseries.co.uk
- You also have the right to complain to the Information Commissioner's Office (ICO): <https://ico.org.uk/concerns/> or to seek a judicial remedy.

