

Kangaroo Kids Record Keeping and Data Protection (GDPR) Policy

February 2025





Statement of Intent

To protect the data and information of all children, families, and staff members across both our settings.

Aim

To ensure our record keeping systems in place for the safe and efficient management of the setting meet legal requirements for the storing and sharing of information within the framework of the GDPR and the Human Rights Act.

Procedures

Children's records are kept in personal files, divided into appropriate sections, and stored separately from their developmental records.

Children's personal files contain other material described as confidential as required, such as Common Assessment Framework assessments, Early Support information or Education, Health and Care Plan (EHCP, case notes including recording of concerns, discussions with parents, and action taken, copies of correspondence and reports from other agencies.

Ethnicity data is only recorded where parents have identified the ethnicity of their child themselves.

Confidentiality is maintained by secure storage of files in a locked cabinet with access restricted.

Staff know how to share information if they believe a child is in need or at risk of suffering harm.

Staff record when and to whom information has been shared, why information was shared and whether consent was given. Where consent has not been given and staff have taken the decision, in line with guidelines, to override the refusal for consent, the decision to do so is recorded.

Guidance and training for staff specifically covers the sharing of information between professions, organisations, and agencies as well as within them, and arrangements for training takes account of the value of multi-agency as well as single agency working.

Records

The following information and documentation are also held:

- name, address and contact details of the provider and all staff employed on the premises
- name address and contact details of any other person who will regularly be in unsupervised contact with children
- a daily record of all children looked after on the premises, their hours of attendance and their named key person
- certificate of registration displayed and shown to parents on request
- records of risk assessments
- record of complaints



Legal references

General Data Protection Regulation 2018

Freedom of Information Act 2000

Human Rights Act 1998

Statutory Framework for the Early Years Foundation Stage (DfE 2021)

Data Protection Act 2018

Further guidance

[Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers](#) (HMG 2018)

Children's records and data protection

During an outbreak of serious illness or disease (such as Covid-19) there may be the need to keep additional records as part of outbreak management. A record is kept of individual cases of children/families who are self-isolating due to symptoms as per usual record-keeping procedures. In all cases the principles of data protection are maintained.

Principles of data protection: lawful processing of data

Personal data shall be:

- a) *processed lawfully, fairly and in a transparent manner in relation to the data subject*
- b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is not compatible for these purposes*
- c) *adequate, relevant and necessary in relation to the purposes for which they are processed*
- d) *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 purpose for which they are processed, are erased or rectified without delay*
- e) *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*
- f) *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 ("integrity and confidentiality")* Article 5 of the General Data Protection Regulations (2018)

Educators should process data, record and share information in line with the principles above.

General safeguarding recording principles

It is vital that all relevant interactions linked to safeguarding children's and



individual's welfare are accurately recorded.

All recordings should be made as soon as possible after the event.

Recording should be to a good standard and clear enough to enable someone other than the person who wrote it, to fully understand what is being described.

Recording can potentially be viewed by a parent/carer or Ofsted inspector, by the successors of the educators who record, and may be used in a family Court as relevant evidence to decide whether a child should remain with their biological parents, or be removed to live somewhere else. Recording needs to be fair and accurate, non-judgemental in tone, descriptive, relevant, and should clearly show what action has been taken to safeguard a child and reflect decision-making relating to safeguarding.

Recording should be complete, it should show what the outcome has been, what happened to referrals, why decisions were made to share or not share information, and it should contain summaries and minutes of relevant multi-agency meetings and multi-agency communication.

If injuries or other safeguarding concerns are being described the description must be clear and accurate and should give specific details of the injury observed and where it is located.

The principles of GDPR and effective safeguarding recording practice are upheld

Recording is factual and non-judgemental.

The procedure for retaining and archiving personal data and the retention schedule and subsequent destruction of data is adhered to.

Parents/carers and children where appropriate are made aware of what will be recorded and in what circumstances information is shared, prior to their child starting at the setting. Parents/carers are issued with 07.1a Privacy notice and should give signed, informed consent to recording and information sharing prior to their child attending the setting. If a parent/carer would not expect their information to be shared in any given situation, normally, they should be asked for consent prior to sharing.

There are circumstances where information is shared without consent to safeguard children. These are detailed below, but in summary, information can be shared without consent if an educator is unable to gain consent, cannot reasonably be expected to gain consent, or gaining consent places a child at risk.

Records can be accessed by and information may be shared with local authority professionals. If there are significant safeguarding or welfare concerns, information may also be shared with a family proceedings Court or the police. Educators are aware of information sharing processes and all families should give informed consent to the way the setting will use, store and share information.

Recording should be completed as soon as possible and within 5 working days as a maximum for safeguarding recording timescales.

If a child attends more than one setting, a two-way flow of information is established between the parents/carers, and other providers. Where appropriate, comments from others (as above) are incorporated into the child's records.



Children's personal files

Appropriate files must be used. These are made of robust card (not ring binders) and have plastic or metal binders to secure documents. File dividers must be inserted into each file.

The sections contained are as follows:

- personal details: registration form and consent forms.
- contractual matters: copies of contract, days and times, record of fees, any fee reminders or records of disputes about fees.
- SEND support requirements
- additional focussed intervention provided by the setting e.g. support for behaviour, language or development that needs an Action Plan at setting level
- records of any meetings held
- welfare and safeguarding concerns: correspondence and reports: all letters and emails to and from other agencies and confidential reports from other agencies

Children's personal files are kept in a filing cabinet, which is always locked when not in use.

- Correspondence in relation to a child is read, any actions noted, and filed immediately
- Access to children's personal files is restricted to those authorised to see them and make entries in them, this being the setting manager, deputy or designated person for child protection, the child's key person, or other staff as authorised by the setting manager.
- Children's personal files are not handed over to anyone else to look at.
- Children's files may be handed to Ofsted as part of an inspection or investigation; they may also be handed to local authority staff conducting a S11 audit as long as authorisation is seen.

Confidentiality, recording and sharing information

Most things that happen between the family, the child and the setting are confidential to the setting. In certain circumstances information is shared, for example, a child protection concern will be shared with other professionals including social care or the police, and settings will give information to children's social workers who undertake S17 or S47 investigations. Normally parents should give informed consent before information is shared, but in some instances, such as if this may place a child at risk, or a serious offence may have been committed, parental consent should not be sought before information is shared. Local Safeguarding Partners (LSP) procedures should be followed when making referrals, and advice sought if there is a lack of clarity about whether or not parental consent is needed before making a referral due to safeguarding concerns.

Staff discuss children's general progress and well-being together in meetings, but more sensitive information is restricted to designated persons and key persons and shared with other staff on a need-to-know basis.



Members of staff do not discuss children with staff who are not involved in the child's care, nor with other parents or anyone else outside of the organisation, unless in a formal and lawful way.

Discussions with other professionals should take place within a professional framework, not on an informal basis. Staff should expect that information shared with other professionals will be shared in some form with parent/carers and other professionals, unless there is a formalised agreement to the contrary, i.e. if a referral is made to children's social care, the identity of the referring agency and some of the details of the referral is likely to be shared with the parent/carer by children's social care.

It is important that members of staff explain to parents that sometimes it is necessary to write things down in their child's file and explain the reasons why.

When recording general information, staff should ensure that records are dated correctly and the time is included where necessary, and signed.

Welfare/child protection concerns are recorded. Information is clear and unambiguous (fact, not opinion), although it may include the educator's thoughts on the impact on the child.

Records are non-judgemental and do not reflect any biased or discriminatory attitude.

Not everything needs to be recorded, but significant events, discussions and telephone conversations must be recorded at the time that they take place.

Recording should be proportionate and necessary.

When deciding what is relevant, the things that cause concern are recorded as well as action taken to deal with the concern. The appropriate recording format is filed within the child's file.

Information shared with other agencies is done in line with these procedures.

Where a decision is made to share information (or not), reasons are recorded.

Staff may use a computer to type reports, or letters. Where this is the case, the typed document is deleted from the computer and only the hard copy is kept.

Electronic copy is downloaded onto a disc, labelled with the child's name and stored in the child's file. No documents are kept on a hard drive because computers do not have facilities for confidential user folders.

The setting is registered with the Information Commissioner's Office (ICO). Staff are expected to follow guidelines issued by the ICO, at <https://ico.org.uk/for-organisations/guidance-index/>

Additional guidance in relation to information sharing about adults is given by the Social Care Institute for Excellence, at www.scie.org.uk/safeguarding/adults/practice/sharing-information

Staff should follow guidance including Working Together to Safeguard Children (DfE 2018); Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers 2018 and What to do if you're Worried a Child is Being Abused (HMG 2015)

Confidentiality definition



- Personal information of a private or sensitive nature, which is not already lawfully in the public domain or readily available from another public source, and has been shared in a relationship, where the person giving the information could reasonably expect it would not be shared with others.

Staff can be said to have a 'confidential relationship' with families. Some families share information about themselves readily; members of staff need to check whether parents regard this information as confidential or not.

Parents sometimes share information about themselves with other parents as well as staff; the setting cannot be held responsible if information is shared beyond those parents whom the person has confided in.

Information shared between parents in a group is usually bound by a shared agreement that the information is confidential and not discussed outside. The setting manager is not responsible should that confidentiality be breached by participants.

Where third parties share information about an individual; staff need to check if it is confidential, both in terms of the party sharing the information and of the person whom the information concerns.

Information shared is confidential to the setting.

Educators ensure that parents/carers understand that information given confidentially will be shared appropriately within the setting (for instance with a designated person, during supervision) and should not agree to withhold information from the designated person or their line manager.

Breach of confidentiality

A breach of confidentiality occurs when confidential information is not authorised by the person who provided it, or to whom it relates, without lawful reason to share.

The impact is that it may put the person in danger, cause embarrassment or pain.

It is not a breach of confidentiality if information was provided on the basis that it would be shared with relevant people or organisations with lawful reason, such as to safeguard an individual at risk or in the public interest, or where there was consent to the sharing.

Procedure 07.1 Children's records and data protection must be followed.

Exception

GDPR enables information to be shared lawfully within a legal framework. The Data Protection Act 2018 balances the right of the person about whom the data is stored with the possible need to share information about them.

The Data Protection Act 2018 contains "safeguarding of children and individuals at risk" as a processing condition enabling "special category personal data" to be processed and to be shared. This allows educators to share without consent if it is not possible to gain consent, if consent cannot reasonably be gained, or if gaining consent would place a child at risk.



Confidential information may be shared without authorisation - either from the person who provided it or to whom it relates, if it is in the public interest and it is not possible or reasonable to gain consent or if gaining consent would place a child or other person at risk. The Data Protection Act 2018 enables data to be shared to safeguard children and individuals at risk. Information may be shared to prevent a crime from being committed or to prevent harm to a child, Information can be shared without consent in the public interest if it is necessary to protect someone from harm, prevent or detect a crime, apprehend an offender, comply with a Court order or other legal obligation or in certain other circumstances where there is sufficient public interest.

Sharing confidential information without consent is done only in circumstances where consideration is given to balancing the needs of the individual with the need to share information about them.

When deciding if public interest should override a duty of confidence, consider the following:

is the intended disclosure appropriate to the relevant aim?

what is the vulnerability of those at risk?

is there another equally effective means of achieving the same aim?

is sharing necessary to prevent/detect crime and uphold the rights and freedoms of others?

is the disclosure necessary to protect other vulnerable people?

The decision to share information should not be made as an individual, but with the backing of the designated person who can provide support, and sometimes ensure protection, through appropriate structures and procedures.

Obtaining consent

Consent to share information is not always needed. However, it remains best practice to engage with people to try to get their agreement to share where it is appropriate and safe to do so.

Using consent as the lawful basis to store information is only valid if the person is fully informed and competent to give consent and they have given consent of their own free will, and without coercion from others, Individuals have the right to withdraw consent at any time.

You should not seek consent to disclose personal information in circumstances where:

- someone has been hurt and information needs to be shared quickly to help them
- obtaining consent would put someone at risk of increased harm
- obtaining consent would prejudice a criminal investigation or prevent a person being questioned or caught for a crime they may have committed
- the information must be disclosed regardless of whether consent is given, for example if a Court order or other legal obligation requires disclosure



- **NB. The serious crimes indicated are those that may harm a child or adult; reporting confidential information about crimes such as theft or benefit fraud are not in this remit.**

Consent

Parents share information about themselves and their families. They have a right to know that any information they share will be regarded as confidential as outlined in our Privacy notice. They should also be informed about the circumstances, and reasons for the setting being under obligation to share information.

Parents are advised that their informed consent will be sought in most cases, as well as the circumstances when consent may not be sought, or their refusal to give consent overridden.

Where there are concerns about whether or not to gain parental consent before sharing information, for example when making a Channel or Prevent referral the setting manager must inform their line manager for clarification before speaking to parents

Consent must be informed - that is the person giving consent needs to understand why information will be shared, what will be shared, who will see information, the purpose of sharing it and the implications for them of sharing that information.

Separated parents

Consent to share need only be sought from one parent. Where parents are separated, this would normally be the parent with whom the child resides.

Where there is a dispute, this needs to be considered carefully.

Where the child is looked after, the local authority, as 'corporate parent' may also need to be consulted before information is shared.

Age for giving consent

A child may have the capacity to understand why information is being shared and the implications. For most children under the age of eight years in a nursery or out of school childcare context, consent to share is sought from the parent, or from a person who has parental responsibility.

Young persons (16-19 years) are capable of informed consent. Some children from age 13 onwards may have capacity to consent in some situations. Where they are deemed not to have capacity, then someone with parental responsibility must consent. If the child is capable and gives consent, this may override the parent's wish not to give consent.

Adults at risk due to safeguarding concerns must be deemed capable of giving or withholding consent to share information about them. In this case 'mental capacity' is defined in terms of the Mental Capacity Act 2005 Code of Practice (Office of the Public Guardian 2007). It is rare that this will apply in the context of the setting.

Ways in which consent to share information can occur



Policies and procedures set out the responsibility of the setting regarding gaining consent to share information, and when it may not be sought or overridden.

Information in leaflets to parents, or other leaflets about the provision, including privacy notices.

Consent forms signed at registration (for example to apply sun cream).

Notes on confidentiality included on every form the parent signs.

Parent signatures on forms giving consent to share information about additional needs, or to pass on child development summaries to the next provider/school.

Further guidance

[Working Together to Safeguard Children](#) (DfE 2018)

[Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers](#) (HMG 2018)

[What to do if you're Worried a Child is Being Abused](#) (HMG 2015)

[Mental Capacity Act 2005 Code of Practice](#) (Office of the Public Guardian 2007)

Privacy notice

Introduction

Personal data is protected in accordance with data protection laws and used in line with your expectations. This privacy notice explains what personal data we collect, why we collect it, how we use it, the control you have over your personal data and the procedures we have in place to protect it.

When we refer to “we”, “us” or “our”, we mean Kangaroo Kids Preschool.

What personal data we collect

We collect personal data about you and your child to provide care and learning tailored to meet your child’s individual needs. Personal details that we obtain from you includes your child’s: name, date of birth, address, and health, development and any special educational needs information. We will also ask for information about who has parental responsibility for your child and any court orders pertaining to your child.

Personal data that we collect about you includes: your name, home and work address, phone numbers, email address, emergency contact details, and family details.



We will only with your consent collect your national Insurance number and date of birth where necessary if you apply for up to 30 hours free childcare and early education. We also collect information regarding benefits and family credits. Please note that if this information is not provided, then we cannot claim funding for your child.

Where applicable we will obtain details of your child's social worker, child protection plans from social care, and health care plans from health professionals and other health agencies.

We may collect this information in a variety of ways. For example, data will be collected from you directly in the registration form; from identity documents; from correspondence with you; or from health and other professionals.

Why we collect personal data and the legal basis for handling your data

We use personal data about you and your child in order to provide childcare and early education services and to fulfil the contractual arrangement you have entered into. This includes using your data in the following ways:

- to support your child's wellbeing and development
- to effectively manage any special education, health or medical needs of your child whilst at the setting
- to carry out regular assessment of your child's progress and to identify any areas of concern
- to maintain relevant contact about your child's wellbeing and development
- to contact you in the case of an emergency
- to process your claim for free childcare and early education, if applicable
- to enable us to respond to any questions you ask
- to keep you updated about information which forms part of your contract with us
- to notify you of service changes or issues

With your consent, we would also like to:

- collect your child's ethnicity and religion data for local authority monitoring purposes
- record your child's activities for their individual learning journal (this will often include photographs of children during play)
- transfer your child's records to the receiving school when s/he transfers

If we wish to use any images of your child for training, publicity or marketing purposes we will seek your written consent for use. You are able to withdraw your consent at any time, for images being taken of your child and/or for the transfer of records to the receiving school, by confirming so in writing to the setting.

We have a legal obligation to process safeguarding related data about your child should we have concerns about her/his welfare.

Who we share your data with

As a registered early years provider in order to deliver childcare and early education services it is necessary for us to share data about you and/or your child with the following categories of recipients:



- Ofsted, when there has been a complaint about the childcare and early education service or during an inspection
- the local authority, if you claim up to 30 hours free child care
- the governments eligibility checker as above, if applicable
- our insurance underwriter, where applicable

We will also share your data:

- if we are legally required to do so, for example, by a law enforcement agency or court
- to enforce or apply the terms and conditions of your contract with us
- to protect your child and other children; for example, by sharing information with medical services, social services or the police
- if it is necessary to protect our rights, property or safety or to protect the rights, property or safety of others
- with the school that your child will be attending, when s/he transfers, if applicable
- if we transfer the management of the setting out or take over any other organisation or part of it, in which case we may disclose your personal data to the prospective seller or buyer so that they may continue using it in the same way

We will never share your data with any organisation to use for their own purposes.

How do we protect your data?

We take the security of your personal data seriously. We have internal policies and strict controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed and to prevent unauthorised access.

Where we engage third parties to process personal data on our behalf, they are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Where do we store your data?

All data you provide to us is stored on secure computers or servers located within the UK or European Economic Area. We may also store paper records in locked filing cabinets.

How long do we retain your data?

- You and your child's data, including registers are retained 3 years after your child no longer uses the setting, or until our next Ofsted inspection after your child leaves our setting.
- Medication records and accident records are kept for longer according to legal requirements.
- Learning journeys are maintained by the setting and available at your request when your child leaves. Records are kept and archived in line with our data retention policy.
- In some cases (child protection or other support service referrals), we may need to keep your data longer, only if it is necessary in order to comply with legal requirements. We



will only keep your data for as long as is necessary to fulfil the purposes it was collected for and in line with data protection laws.

Your rights with respect to your data

As a data subject, you have a number of rights. You can:

- request to access, amend or correct the personal data we hold about you and/or your child
- request that we delete or stop processing your and/or your child's personal data, for example where the data is no longer necessary for the purposes of processing or where you wish to withdraw consent
- request that we transfer your and your child's personal data to another person

If you wish to exercise any of these rights at any time please contact the manager at the setting.

How to ask questions about this notice

If you have any questions, comments or concerns about any aspect of this notice or how we handle your data please contact the manager at the setting.

How to contact the Information Commissioner Office (ICO)

If you are concerned about the way your data is handled and remain dissatisfied after raising your concern, you have the right to complain to the Information Commissioner Office (ICO). The ICO can be contacted at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or <https://ico.org.uk/>.