9. Data Protection, Record keeping and Confidentiality Policy

Name of Responsible Person: All staff

All information on children and adults held by Tigers Day Nurseries will be treated confidentially and stored securely. Information will be checked regularly to ensure we have up to date and accurate records. This is particularly important for information such as emergency contact numbers for children in our care. All parents and carers are asked to inform the setting immediately should any of their personal details change. We seek signed permission from parents and carers to hold and store information on their child and family and information shared with any other agencies is done with written permission from parents and carers.

We have a Data Protection Officer (The Operations Manager) who is responsible for monitoring and updating Tigers processing policies, procedures and practices, will report any breaches to the ICO (Information Commissioners Office), maintain a breach register and complete privacy impact assessments where required. All our staff in the settings are Data Protection Processors as they have access to data on children and their families and will receive training to understand their obligations and responsibilities for protecting data shared in the setting.

Confidentiality underpins the relationship of trust that exists between staff and parents. The need for confidentiality in discussing issues relating to children and their families is impressed on staff during their induction period and revisited periodically with the entire staff team. If any staff member is in doubt about whether an issue is confidential, they must discuss this with their Manager. No information or contact details for any child, parent, carer or member of staff is given out over the telephone under any circumstances. Parents who request other parent's details are asked to give permission for their own to be passed on instead.

Lists, records and attendance sheets are produced to support different aspects of the work of the setting. It is the responsibility of the staff to complete these promptly and accurately and to ensure they are stored safely. This is essential for registers of attendance and staff signing in records. Written records are made of all meetings as well as incidents and accidents and will be stored securely within the setting. All staff are made aware of the need to record accurate and factual information and understand the purpose for which different types of records may be kept.

Permission will be sought from parents/carers to share information on their child with other agencies and professionals involved in their child's care. Private and personal information would only be shared in exceptional circumstances without parental permission such as if it is believed a child is in immediate danger of harm.

In the interests of equality and freedom of information, as much information as possible about the vision, values, aims, objectives and day to day running of the nursery is made freely available to parents/carers and staff.

Procedures:

Storage of Confidential Information

Sharing of Confidential Information

Disposal of Confidential Information

Credit, Debit and Visa card payment information

Controls on Information Technology and Privacy

Staff Procedure for Mobile Phones and Camera Use

Sending group emails

Storage of Confidential Information

- Only relevant information will be sought from parents/carers and stored
- Personal information regarding children and their families, and staff records are stored in locked filing cabinets or on our secure online system which is password protected.
- Information is given out only on a 'need to know' basis
- Once information is no longer required it is placed in secure storage in archive files for the legal amount of time if required, or shredded.
- Archiving of child/family information is stored using legislation from the Childcare Act 2006 as follows: medical records on the child 30 years, accident reports 21 years 3 months, permission to administer medicine 21 years, 3 months, emergency treatment permission 21 years 3 months, registers 21 years, accident reports 21 years, collection authority 21 years, records reported under RIDDOR 3 years, parent contact details 2 years, details about child 2 years, outing permission 2 years.
- Inspection evidence used during an Ofsted inspection must be retained for longer than 6 years if:
  - Any action relates to safeguarding
  - The setting is being monitored or regulatory action is linked to the inspection.
  - There is a potential or current litigation claim against Ofsted such as a judicial review.
  - The inspection is of a very sensitive nature or is likely to be of regional importance due to a high level of political or press interest.

- There is an appeal against enforcement action or an ongoing complaint.
- It has been identified for research or evaluation purposes.

- Marketing material which includes children's images with permission from their parents will be updated every five years and old images destroyed.
- Children's photos on Facebook will be stored infinitely and we will ensure parents give us permission before using any child's image.
- Children and family details are stored securely on our online management program Connect which parents can access through ParentZone. Once a child has left the setting the Managers will make those children 'inactive' on the system which means nothing else can be added by the setting but parents can still access their child's learning journey on their app.
- If parents requested all records of the child can be deleted from Connect aside from the child's name, address and medical records and will show on the system as 'anon'. If parents would like this it needs to be requested individually by emailing the Operations Manager opsmanager@tigersdaynurseries.co.uk

Sharing of Confidential Information

- Personal information is to be shared only with permission from parents/carers with relevant outside agencies and professional involved in the child's care, unless there is strong evidence the child is at risk of significant harm and then relevant information on the child can be shared with the relevant authorities without first seeking parental permission.
- No information is shared over the telephone, only written information or emails which are password protected.
- Staff references are usually only accepted in written form and are followed up with a telephone call to establish credibility and accuracy. The Operations Manager can decide to accept a telephone reference at her discretion.
- References for staff who have left us are completed only by The Operations Manager and only basic details completed.
- Parents/carers are not given confidential information regarding any other child within the setting and identities of children are kept anonymous.
- Parents/carers who request contact numbers etc of other parents are asked to leave their own details to be passed on if wished.
- Any breach of personal data will be reported to the Independent Commissioners Office (ICO) within 72 hours of the discovery of the breach. All those involved will be informed.

Disposal of Confidential Information

- Once information on a child, parent/carer or staff member is no longer required it is placed in secure storage on the premises or shredded if no longer relevant.
- This is stored for a maximum of 3 years in the setting before being archived in secure storage off the premises.
- Information that is no longer required is shredded if it contains any information that could be used to identify a child, parent/carer or staff member.

Credit, debit and Visa card information

- If parents use credit, debit or Visa cards to pay for their fees, we do not store any of this information for future use.
- Credit, debit or Visa card machines are linked to each setting so parents/carers are able to pay for their child's fees at their own setting.
- We do not hold or store any credit, debit or Visa card information given to us over the telephone for card payments.
- We do not store any credit, debit or Visa card information in parents file or on our online Connect system.
- Any information given over the telephone while making a card payment is immediately destroyed after use.
- Parents/carers who use the credit, debit or Visa card machines in their child's setting are issued with a receipt, either from the machine itself, or if they use contactless payment (for under £100) the Manager will issue a written receipt for this payment.
- Our own receipts for these payments are stored on site, or in our accounts office until the payment is cross referenced into the bank accounts and then they are destroyed.

Controls on Information Technology and Privacy

- Staff are forbidden to have their own mobile phones on their person during working hours. They are permitted to use them in their breaks.
- Staff will have text, camera and call function on any smart watch disabled while they are on duty.
- The nursery mobile is used during walks and trips out. This is not able to take photos.
- The nursery has its own tablets for each base room which are used to record children's progress and events and upload these to iConnect, our secure online system for children's records and learning journals.
- Screen time:

- As a setting we are aware that even the very youngest of our children have access to online data and media, so therefore any use of technology in our settings is used for educational purposes and is limited.
- We have giant ipad screens which we use to support children's communication. language, EAL and children's learning of mathematics and literacy.
- We do not have TV screens in our settings, but the children will occasionally have a 'digital story' as an activity.
- Screen time for all our children is limited to 30 minutes at once, for a maximum of twice a day.
- Children have access to hand-held computers and programmable toys which staff monitor the use of.
- We have web blockers to ensure the children and staff can only access suitable content on the settings computers and hand-held devices.
- We provide the children with simple, age appropriate information on safe use of digital technology and also share this with parents.

- Staff are not able to access children's learning journals off the premises and we have systems in place to check this. If this ever is required the Operations Manager will provide permission in certain individual circumstances.
- The secure Connect system is used to maintain information on the children, their parents/carers and staff. It is also used to send monthly invoices, account statements and to send regular email updates to parents.
- Only those with a secure password are able to access Connect and iConnect and the Operations Manager will set up accounts for staff as required.
- Parents/carers are asked to indicate which of them they would like to be set up as the 'bill payer' and this contact will receive the monthly invoices sent from the accounts department.
- If there is a failure of the Connect system, invoices or memos etc will be printed and given out to parents/carers on drop off or collection.
- Staff who use social network such as 'Facebook' or 'Twitter' will not make reference to the nursery or show images of themselves wearing their uniform.
- We advise staff members not to 'add' parents as 'friends' on social network sites.
- The Senior Manager and Marketing Manager are responsible for updates/news from the nurseries placed on Facebook. This media can be used to inform parents/carers of anything urgent happening at the setting e.g. roadworks nearby or restricted parking on site.
- Any conduct on social network sites which could bring the nursery into disrepute is classed as gross misconduct and could result in staff dismissal.

- All staff are subject to an exit interview when they leave the setting and are reminded of the data protection and confidentiality guidance agreed as part of their contract of employment.

Staff Procedure for Mobile Phones and Camera Use

- Staff mobile phones are stored in their lockers during working hours and are accessed only on staff breaks.
- Calls, text and camera functions on staff smart watches are disabled while they are on duty.
- Staff phones and cameras are not permitted in areas where the children are present at any time.
- The nursery has an allocated phone for staff to use during walks and trips out.
- Photographs taken using the nursery tablets are not to be downloaded onto staff computers.
- Photographic images of the children are downloaded onto the tablets and are sent electronically to the parents using a secure, password protected system. All images and observations on the child are first checked by the Managers to ensure they are appropriate.

Sending Group emails

- Group emails should be sent on our Connect system where possible as this offers the best level of security
- If this is not possible group emails should be sent out by members of the management team, including third in charge staff.
- Group emails must be sent using the bcc facility to ensure recipients cannot see others email addresses.
- If any mistakes are made with this process they need to be reported to the Operations Manager immediately to ensure the least amount of damage is incurred. Advice can be sought from the ICO by calling their helpline. If a data breach needs to be reported they can assist and guide. Data breaches must be reported to the ICO within 72 hours.

Updated November 2023