Record Keeping Policies

Little Wombatz

26/03/2018
Chris Barton

Children's records

Policy statement

There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the General Data Protection Regulations, Data Protection Act, the UN Convention for the Rights of the Child and the Human Rights Act. This policy and procedure is taken in conjunction with the Confidentiality and Client Access to Records policy and Information Sharing policy.

Procedures

We keep two kinds of records on children attending our setting:

Developmental records

- These include observations of children in the setting, photographs, video clips and samples of their work and summary developmental reports.
- Formative assessments are kept using the online system "Tapestry" and parents can access their child's record whenever they wish using the secure password and username provided by Tapestry.
- Summative records are kept on paper and stored in the work filing cabinet, securely when the setting is not open. Parents may ask to see these whenever they wish and the contents will be uploaded onto Tapestry twice annually as part of the reporting system.

Personal records

- These include registration and admission forms, signed consent forms, and correspondence concerning the child or family, reports or minutes from meetings concerning the child from other agencies, an ongoing record of relevant contact with parents, and observations by staff on any confidential matter involving the child, such as developmental concerns or child protection matters.
- These confidential records are stored in a lockable filing cabinet and are kept secure at the registered office. Files needed on a daily basis are stored in a locked filing cabinet at the Scout & Guide Hall.
- Parents have access, in accordance with our Client Access to Records policy, to the files and records of their own children but do not have access to information about any other child. Parents may request to see all the information held about their child. This will be made available within one month of the request being received in writing.
- Staff will not discuss personal information given by parents with other members of staff, except where it affects planning for the child's needs. Staff induction includes an awareness of the importance of confidentiality in the role of the key person.

- We retain children's records for three years after they have left the setting. These are kept in a secure place.

Other records

- Issues to do with the employment of staff, whether paid or unpaid, remain confidential to the people directly involved with making personnel decisions.
- Students on recognised qualifications and training, when they are observing in the setting, are advised of our confidentiality policy and are required to respect it.

Provider records

Policy statement

We keep records for the purpose of maintaining our business. These include:

- *Records pertaining to our registration with Ofsted and the county council.*
- *Records relating to the hire of the hall and other contractual documentation pertaining to amenities, services and goods.*
- *Financial records pertaining to income and expenditure.*
- *Risk assessments.*
- *Employment records of staff.*

Our records are regarded as confidential based on sensitivity of information, such as with regard to employment records and these are maintained with regard to the framework of the General Data Protection Regulations, Data Protection Act and the Human Rights Act.

This policy and procedure is taken in conjunction with the Confidentiality and Client Access to Records policy and Information Sharing policy.

Procedures

- All records are the responsibility of the manager who ensure they are kept securely.
- All records are kept in an orderly way in files and filing is kept up-to-date.
- Financial records are kept up-to-date for audit purposes and financial records submitted annually to HMRC and Companies House.
- Health and safety records are maintained; these include risk assessments, details of checks or inspections and guidance etc.
- Our Ofsted registration certificate is displayed.
- Our Public Liability insurance certificate is displayed.

- All our employment and staff records are kept securely and confidentially in a locked filing cabinet at the registered office address.
- Staff records are destroyed six years after a member of staff has left the setting.

Transfer of records to school

Policy statement

We recognise that children sometimes move to another early years setting before they go on to school although many will leave our setting to enter a nursery or reception class.

We prepare children for these transitions and involve parents and the receiving setting in this process. We prepare records about a child's development and learning in the EYFS in our setting; in order to enable smooth transitions, we share appropriate information with the receiving setting or school at transfer.

Confidential records are shared where there have been child protection concerns according to the process required by our Local Safeguarding Children Board.

The procedure guides this process and determines what information we can and cannot share with a receiving school or setting.

Procedures

Transfer of development records for a child moving to another early years setting or school

- Using the EYFS assessment of development and learning ensure the key person prepares a summary of achievements in the six areas of learning.
- This record refers to any additional language spoken by the child and his or her progress in both languages.
- The record also refers to any additional needs that have been identified or addressed by the setting.
- The record also refers to any special needs or disability and whether a CAF was raised in respect of special needs or disability, whether there is a Education, Health and Care Plan and gives the name of the lead professional.
- The record contains a summary by the key person.
- The document may be accompanied by other evidence such as photos or drawings that the child has made.
- For transfer to school we use the Tapestry summative assessment document. If the school or receiving setting also use tapestry we arrange for the transfer of the entire file, using the Tapestry secure file sharing system.

- If there have been any welfare or protection concerns a dot is placed on the front of the assessment record.

Transfer of confidential information

- The receiving school or setting will need to have a record of concerns that were raised in the setting and what was done about them.
- A summary of the concerns will be made to send to the receiving setting or school along with the date of the last professional meeting or case conference.
- Where a CAF has been raised in respect of any welfare concerns the name and contact details of the lead professional will be passed on to the receiving setting or school.
- Where there has been a S47 investigation regarding a child protection concern the name and contact details of the child's social worker will be passed on to the receiving setting or school – regardless of the outcome of the investigation.
- This information is posted or taken to the school or setting, addressed to the setting or school's designated person for child protection and marked confidential.

Confidentiality and client access to records

Policy statement

Definition: 'Confidential information is information that is not normally in the public domain or readily available from another source, it should have a degree of sensitivity and value and be subject to a duty of confidence. A duty of confidence arises when one person provides information to another in circumstances where it is reasonable to expect that the information will be held in confidence.' (Information Sharing: Guidance for Practitioners and Managers (DCSF 2008))

At Little Wombatz, staff and managers can be said to have a 'confidential relationship' with families. It is our intention to respect the privacy of children and their parents and carers, while ensuring that they access high quality early years care and education in our setting. We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the General Data Protection Regulations, the Data Protection Act and the Human Rights Act.

Confidentiality procedures

- We always check whether parents regard the information they share with us to be regarded as confidential or not.
- Some 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 discussion or training group is usually bound by a shared agreement that the information is confidential to the group and not discussed outside of it.
- We inform parents when we need to record confidential information beyond the general personal information we keep (see our record keeping procedures) - for example with regard to any injuries, concerns or changes in relation to the child or the family, any discussions with parents on sensitive matters, any records we are obliged to keep regarding action taken in respect of child protection and any contact and correspondence with external agencies in relation to their child.
- We keep all records securely (see our record keeping procedures).

Client access to records procedures

Parents may request access to any confidential records held on their child and family following the procedure below:

- Any request to see the child's personal file by a parent or person with parental responsibility must be made in writing to the manager.
- The setting commits to providing access within 30 days.
- The setting's manager prepares the file for viewing.
- All third parties are written to, stating that a request for disclosure has been received and asking for their permission to disclose to the person requesting it. Copies of these letters are retained on file.
- 'Third parties' include all family members who may be referred to in the records.
- It also includes workers from any other agency, including social services, the health authority, etc. It is usual for agencies to refuse consent to disclose, preferring the individual to go directly to them.
- When all the consents/refusals to disclose have been received these are attached to the copy of the request letter.
- A photocopy of the complete file is taken.

- The manager and a deputy manager go through the file and remove any information which a third party has refused consent to disclose. This is done with a thick black marker, to score through every reference to the third party and information they have added to the file.
- What remains is the information recorded by the setting, detailing the work initiated and followed by them in relation to confidential matters. This is called the 'clean copy'.
- The 'clean copy' is photocopied for the parents who are then invited in to discuss the contents. The file will not be given straight over, but will be gone through by the setting leader, so that it can be explained.
- Legal advice may be sought before sharing a file, especially where the parent has possible grounds for litigation against the setting or another (third party) agency.

All the undertakings above are subject to the paramount commitment of the setting, which is to the safety and well-being of the child. Please see also our policy on child protection.

Information sharing

"Practitioners need to understand their organisation's position and commitment to information sharing. They need to have confidence in the continued support of their organisation where they have used their professional judgement and shared information professionally."

Information Sharing: Guidance for Practitioners and Managers (DCSF 2008)

Policy statement

We recognise that parents have a right to know that information they share will be regarded as confidential as well as be informed about the circumstances, and reasons, when we are obliged to share information.

We are obliged to share confidential information without authorisation from the person who provided it or to whom it relates if it is in the public interest. That is when:

- it is to prevent a crime from being committed or intervene where one may have been, or to prevent harm to a child or adult; or
- not sharing it could be worse than the outcome of having shared it.

The decision should never be made as an individual, but with the back-up of management. A manager will not take a decision on their own but will always consult with a deputy manager or the setting SENCO before sharing information. The three critical criteria are:

- Where there is *evidence* that the child is suffering, or is at risk of suffering, significant harm.
- Where there *is reasonable cause to believe* that a child may be suffering, or at risk of suffering, significant harm.

- To *prevent* significant harm arising to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime.

Procedures

Our procedure is based on the 7 golden rules for information sharing as set out in *Information Sharing: Guidance for Practitioners and Managers (DCSF 2008).*

1. Remembering that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately. *Our policy and procedures on information sharing provide guidance to appropriate sharing of information with external agencies.*
2. Being open and honest. Explaining to families how, when and why information will be shared about them and with whom. Seeking consent to share information, unless it puts the child at risk or undermines a criminal investigation. *In our setting, we ensure parents:*
   - *receive information about our information sharing policy when starting their child in the setting and they sign a form to say that they understand circumstances when information may be shared without their consent. This will only be when it is a matter of safeguarding a child or vulnerable adult. This is on our registration form;*
   - *have information about our Safeguarding Children and Child Protection policy; and*
   - *have information about the circumstances when information will be shared with external agencies, for example, regarding any special needs the child may have or transition to school.*
3. Seeking advice when there are doubts about possible significant harm to a child or others. *Managers contact children's social care for advice on a "what if" basis where they have doubts or are unsure.*
4. Sharing with consent where appropriate. Respecting the wishes of children and parents not to consent to share confidential information. However, in the interests of the child, know when it is reasonable to override their wish. *Guidelines for consent are part of this procedure.*
5. Managers are conversant with this guidance and can advise staff accordingly. They consider the safety and welfare of the child when deciding about sharing information – if there are concerns regarding 'significant harm' the child's well-being and safety are paramount. *In our setting, we:*
   - *record concerns and discuss these with the setting's designated person for child protection matters. Record decisions made and the reasons why information will be shared and to whom; and*
   - *follow the procedures for reporting concerns and record keeping.*

6. Information shared will be accurate and up-to-date, necessary for the purpose it is being shared for, shared only with those who need to know and shared securely. *Our Child Protection procedure and Record Keeping procedure set out how and where information should be recorded and what information should be shared with another agency when making a referral.*
7. Reasons for decisions to share information, or not, are recorded. *Provision for this is set out in our Record Keeping procedure*

Consent

- Parents have a right to be informed that their consent to share information will be sought in most cases, as well as the kinds of circumstances when their consent may not be sought, or their refusal to give consent may be overridden. We do this as follows: Our policies and procedures set out our responsibility regarding gaining consent to share information and when it may not be sought or overridden.
- We may cover this verbally when the child starts or include this in our prospectus.
- Parents sign a form at registration to say they understand this.
- Parents are asked to give written consent to share information about any additional needs their child may have, or to pass on child development summaries, to the next provider/school.
- Copies are given to parents of the forms they sign.

We consider the following questions when we need to share:

- Is there legitimate purpose to sharing the information?
- Does the information enable the person to be identified?
- Is the information confidential?
- If the information is confidential, do you have consent to share?
- Is there a statutory duty or court order to share information?
- If consent is refused, or there are good reasons not to seek consent, is there sufficient public interest to share information?
- If the decision is to share, are you sharing the right information in the right way?
- Have you properly recorded your decision?

All the undertakings above are subject to the paramount commitment of the setting, which is to the safety and well-being of the child. Please also see our Safeguarding Children and Child Protection policy.

Data Transporting Policy

This policy sets out the way in which personal or sensitive data must be transferred by or on behalf of Little Wombatz Ltd, whether it is held on paper or electronically. The policy is applicable to Little Wombatz employees, contractors, volunteers, students and other organisations or agencies working for or on behalf of the company.

Little Wombatz Ltd is committed to securely handling the personal data of children, and staff. The Data Protection Act (1998) requires all organisations to take "Appropriate technical and organisational measures …. against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

This policy should be read in conjunction with the Safeguarding and Record Keeping Policies.

1. Understanding personal and sensitive personal data.

This policy refers to 'personal' or 'sensitive personal' data.

1.1 Staff must identify personal data

Personal data includes any data that relates to a living individual, or which could identify an individual. It can also include any contextual data about individuals that when combined with other data will identify an individual. Personal data also includes any expression of opinion about the individual and any indication of the intentions of the company, or any other person, in respect of that individual. This could include letters, correspondence, spreadsheets, photographs, learning journeys or notebooks that contain the names or full addresses of the children, families or staff.

1.2 Staff must identify sensitive personal data

Sensitive personal data is also data that can identify a living person, but which includes additional information relating to the following areas:

(a) a person's racial or ethnic origin;
(b) political opinions;
(c) religious beliefs or other beliefs of a similar nature;
(d) membership of a trade union;
(e) physical or mental health or condition;
(f) sexual life;
(g) the commission or alleged commission of any criminal offence; or
(h) any criminal proceedings for any offence committed or alleged to have been committed the disposal of such proceedings or the sentence of any court in such proceedings.

1.3 Staff must identify Restricted data

Any information that links an identifiable individual with information that, if released, would put them at significant risk of harm or distress will be considered Restricted and must be transported securely. Personal data will be considered Restricted where such data is likely to:

a) Cause substantial distress to individuals
b) Cause adverse embarrassment to an organisation
c) Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies
d) Prejudice the investigation or facilitate the commission of crime
e) Breach proper undertakings to maintain the confidence of information provided by third parties
f) Impede the effective development or operation of government policies
g) Breach statutory restrictions on disclosure of information
h) Disadvantage government in commercial or policy negotiations with others
i) Undermine the proper management of the public sector and its operations.

2 Guidelines for transporting personal data

a) Data must be transported directly to the where it is required
b) Any data must not be left unattended while being transported
c) Data must be anonymised wherever possible before it is removed from company premises
d) If it is possible, paper should be shredded or securely disposed of at destination
e) Where (d) is not possible sensitive paper documents should be returned to company premises to be securely destroyed.
f) Data must be stored according to the data protection act, in a locked box accessible only to the staff member.
g) Laptops and ipads must be locked with a passcode known only to staff members.

2.1 Transporting data by mail

a) The name address and postcode of the recipient must be confirmed prior to posting
b) All mail must be sealed in a robust envelope
c) Sensitive personal data must only be sent by the Royal Mail Recorded Delivery service.
d) When sending sensitive personal data, mail must be marked 'Private and Confidential. To be opened by Addressee only'
e) If the risk is thought to be exceptional, a courier should be used.

2.2 Transporting data by phone

Disclosing personal data over the phone can present a serious security risk, which all staff members must
address.
Two principles MUST apply when disclosing personal data over the phone:
(i) All routine disclosures must have a written record and be signed by two members of staff
(ii) All other disclosures of personal data by phone must comply with the standards set out below.
If a member of staff receives a request for personal or confidential information by phone, they must:
a) Confirm the name, job title and organisation of the person requesting the information.
b) Take a contact number – this should be a main switchboard number and not a mobile or direct line
c) Document any data disclosed over the phone and record the reason why.

2.3 Transporting data by email

a) The email address must be confirmed by the recipient prior to sending, preferably by sending an initial email.
b) Wherever possible a Manage file transfer (MFT) should be arranged.
c) If this is not possible personal data should be transferred using a Dropbox or similar file sharing system
d) Email trails should be kept for auditing purposes.

2.4 Personal data that is transported should be protectively marked

Any personal data that is transported should be protectively marked. An example of this is marking a letter containing sensitive data as 'Confidential'. This does not prevent a third party from reading it but does help indicate what the third party might do with the letter should they access it in error. Personal data being transported should contain a letter detailing what to do if it is found.

2.5 Data Transport risks must be documented

Each method of transporting data carries its own risks which need to be mitigated. See Appendix A for risk assessment.

3 Reporting Data Loss or Breach

It is the duty of all users to immediately report any actual or suspected breaches in information security to the owner as soon as possible. The owner will then carry out a further risk assessment and decide what action needs to be taken, such as reporting the breach to the information commissioner's office.

APPENDIX A: Transferring Data Risk Assessment

Risk	Action to mitigate risk	Further Action to take
With a third-party Supplier company data could be accessed or misused by unauthorised users	Ensure that an appropriate contractual agreement sets out roles and responsibilities for managing sensitive data	
With a partner agency company data is not being shared legally	Develop a sharing protocol which evidences the legal basis for sharing and the provisions for safe and compliant data transport	
Data could be viewed by unauthorised parties	Named recipients should be defined in any sharing protocol	
Via email Email could be viewed by unauthorised parties	Email should only be sent to named recipients and not generic email addresses	
Email could be hacked into	Secure email channels should be used to transport data	
Data could be lost or stolen	- Take appropriate steps to manage the data effectively - Avoid unnecessary journeys with the data - Do not leave data unattended in public places or visible in cars or bags.	
Via hard copy Post could be intercepted or lost	Use registered mail	

Tapestry Policy

Statement of intent

At Little Wombatz we use an online system called Tapestry to record and store all observations and assessments relating to each child. This is a safe and secure system and one that enables parents and carers to access their child's learning journey at any time. They can share it with their child, family and friends at home and also post any comments and photographs of their own, helping to create a fully holistic view of the child and strengthen the parent partnership. We aim to add at least one Key Person observation within a fortnightly cycle for each child to contribute to our observe-assess-plan cycle.

Safety and security

Staff use tablets to take the photographs for observations which are be uploaded to the journals. Each staff member has a secure login which is password and pin protected. The tablets are kept in a secure cupboard at pre-school and may only be taken home by staff members for specific reasons and with the express consent of management. Photographs are deleted from the tablets once they have been uploaded to Tapestry.

Staff will be allocated time at work to update journals and assess their key children's next steps. Staff should have minimal need to work on journals at home but if they wish to do so they must take home a setting tablet to work on. Staff are not permitted to access Tapestry on their own devices. Tablets must be pin protected and have had all photographs removed from their internal storage before transporting. They must be transported and stored in line with the setting's Data Transfer Policy.

If staff do work on Tapestry at home they should be aware of any other people around them and make sure they are not overlooked. They must logout as soon as they have stopped working.
If any member of staff suspects that their login details have been compromised in any way, they must inform the pre-school managers immediately and new login details will be created to block access to the account.

The Tapestry on-line Learning Journey system is hosted on secure dedicated servers based in the
UK. All data held on our Tapestry account is owned by Little Wombatz; we are registered controllers of data with the Information Commissioner's Office and are bound by the Data Protection Act.

Parents

Parents logging in to the system can only access their own child's Learning Journey. Parents may input new observations and photo's, and add comments to existing observations. They do not have the necessary permission to edit existing content. Parents are asked to sign a consent form giving permission for their child's image to appear in other children's Learning Journeys, and to protect images of other children that may appear in any photos contained in their child's Learning Journey. If parents withhold this consent their child is only ever photographed alone and no shared observations are made including that child.

Parents without internet
For parents without access to the internet, we will print all the information from Tapestry and collate it into a paper Learning Journey. This will be in the setting for the parent to view when requested in advance and will be available to take home when the child leaves the setting.

When children leave
When children move to another setting we will transfer the Tapestry account to the new setting, if they also use Tapestry. If they do not, we will email a PDF to the setting.

When a child leaves the setting to start school we will email the parents a PDF copy of their child's
Learning Journey so they have a lasting record of their child's time at pre-school. The child's information, and their Learning Journey will be permanently deleted from our Tapestry account so that no data on that child will remain with us once they have left.

Staff Tapestry Code of Conduct

- I understand and agree that my tapestry login and is strictly only for my use
- The login and content cannot be shared with anyone outside of Little Wombatz
- The content cannot be downloaded or discussed outside of Little Wombatz
- Any content printed for internal use from the system must be shredded when finished with
- I understand my password must not be saved on any device
- I understand I must ensure I have logged out properly after each session
- I understand I must not access Tapestry from my personal devices
- I understand that when using Tapestry outside of the setting I need to be aware of my surroundings to ensure that the material is kept confidential