KIDS CLUB ELY LTD
St John's Preschool

Data Transporting Policy

This policy sets out the way in which personal or sensitive data must be transferred by or on behalf of Kids Club Ely Ltd & St John's Preschool, whether it is held on paper or electronically. The policy is applicable to Kids Club Ely Ltd employees, contractors, volunteers, students and other organisations or agencies working for or on behalf of the company.

Kids Club Ely Ltd & St John's Preschool 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	