



Data Protection Policy

This policy defines the arrangements within York Childcare Ltd (YCL) to ensure compliance with the requirements of The Data Protection Act, 1998.

Introduction

The Data Protection Act outlines requirements for all organisations which collect and process personal data.

Personal data is defined as any information relating to an 'identifiable living individual' and is therefore applicable to children, parents and carers, employees, trustees, volunteers, students and suppliers.

The Data Protection Act applies to any information recorded in a filing system which allows personal data to be accessed.

The Data Protection Act applies to records kept both in hard copy (paper) format, and in computer files.

Principles of data protection

YCL is committed to the enforcement of the following code of good practice in relation to the data it keeps on children, parents and carers, employees, trustees, volunteers, students and suppliers. All data will:

- Be fairly and legally processed
- Be relevant to the needs of the nursery setting
- Not be unnecessarily excessive in detail
- Be accurately maintained
- Not be kept longer than necessary
- Be used in accordance with the rights of each individual
- Be stored securely
- Archived in accordance with YCL's Safe Storage Policy
- Securely destroyed / deleted in accordance with YCL's Safe Storage Policy.

The following policies are also relevant:

- Confidentiality Policy
- IT Policy
- Safeguarding Policy
- Safe Storage Policy

Policy details

In order for personal data to be collected and processed, YCL will require written consent from each individual or, in the case of children, from their parent or carer.

It will be considered that consent is provided from nursery users by the parent or carer by completing the nursery registration form and associated consent forms for their child/children. It will be considered that consent is provided from employees by completing the job application form at the onset of employment, and where the employee has not registered an objection to their data being used.

All individuals have the right of access to manual and computerised records concerning their personal data.

Where it is deemed necessary to divulge data to a third party this will only be done with the express permission of the individual subject, unless this could be considered as a justifiable action in connection with a safeguarding concern, or under the instruction of a legally binding enforcement order.

Personal data and records are maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure. Records may be held in hard copy (paper) format and as computer files.

Particular attention is paid to the following aspects regarding storage.

Hard copy files:

- Files are kept in a locked cabinet within secure premises where access is not possible for unauthorised persons
- Senior nursery staff, administrative staff and staff with keyperson responsibilities have access to children's and to parent's / carer's details when required as a part of their work duties
- The general manager, administrative staff and the nursery manager (or person acting with managerial responsibility) have access to staff details

Computer files:

- Files containing sensitive data are stored where passwords are required
- Nursery PCs and tablets are set up so that passwords are required to open them
- YCL will only use reputable systems and sites for cloud storage (eg Tapestry for recording and tracking children's progress)
- Back-up systems follow the same protocol

When personal data is being processed, staff take reasonable precautions to prevent sighting of data by unauthorised persons:

- Documents containing personal data are locked away when not in use
- Where practical, computer VDU screens are tilted towards the user and away from the general office environment
- VDUs are not left on when not in use and are password protected (see IT Policy)