



Policies and Procedures

These policies were adopted on	Signed on behalf of the pre-school	Date for overall review (individual policies will be reviewed as needed. See list of policies for dates)
August 2023	Yve Puxty (Manager)	September 2024



5. Information and Records Policies and Procedures		
5.1 Confidentiality		
5. General Data Processing Regulations (GDPR)		
5.3 Comments and Complaints		
5.4 Complaints Record (sample)		
5.5 Admissions and settling In (transitions)		



5. Information and Records Policies and Procedures

5.1 Information and Records Policies and Procedures - Confidentiality

Information received by the setting is often confidential. To maintain parents' confidence in our professional approach to this information Netherfield Pre-school ensures:-

- All parents can see the details kept about their child and themselves at any time.
- Parents will not be given access to information kept about other children.
- Feedback given to parents on their child's progress will be given directly to the parents unless they state that a third party can be involved.e.g.childminder or nanny.
- Information about a child's medical needs or status i.e. HIV or concerns about Child Protection issues will be kept in a separate file and will only be made available to authorized personnel on a need to know basis.
- Staff, students and visitors to the setting will be made aware of the importance of confidentiality of information and their responsibility within the setting.
- Information about individual members of staff will not be given out to anyone without the permission of the person except in cases of child Protection.



5.2 Information and Records Policies and Procedures - General Data Processing Regulations (GDPR)

Policy Statement

GDPR came into effect on 25 May 2018, and it replaced current the Data Protection Act (DPA) legislation. It is intended to provide greater transparency around the collection and use of data. The scheme will be governed by the Information Commissioner's Office (ICO). We are registered with the ICO (Information Commissioners Office) under registration Z253129X

GDPR states that personal data should be 'processed fairly & lawfully' and 'collected for specified, explicit and legitimate purposes' and that individual's data is not processed without their knowledge and are only processed with their 'explicit' consent.

Netherfield Pre-school aims to ensure that all personal data collected about staff, children, parents, carers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format. The six principles of GDPR are that data is:

1. Processed fairly, lawfully and in a transparent manner
2. Used for specified, explicit and legitimate purposes
3. Used in a way that is adequate, relevant and limited
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed in a manner that ensures appropriate security of the data

Under GDPR people will continue to have the right to a Freedom of Information request (FOI) – from bodies dealing with public money or a Subject Access Request (SAR) - anyone can request data from anyone else.

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of personal information.

GDPR Definitions

Personal data

Any information either digital or hard copy relating to an identified, or identifiable, individual. This may include the individual's name (including initials), address, phone number, online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.



Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, sexual orientation.

Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject

The identified or identifiable individual whose personal data is held or processed.

Data Officer

A person or organisation that determines the purposes and the means of processing of personal data.

Data processor

A person or other body, other than an employee of the data officer, who processes personal data on behalf of the data officer.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Netherfield Pre-school's Obligations Procedures for GDPR

- **ICO** – Netherfield Pre-school is registered with the ICO (Information Commissioners Office) under registration reference: Z253129X. Our current certificate is on display in the main entrance hallway next to the front door.
- **Individual rights** — Netherfield Pre-school acknowledges that individuals will have new and enhanced rights on the collection, access and erasure of their data. We will ensure our pre-school has systems and processes in place that promotes these rights.
- **Privacy notices** — When we collect any data we will be transparent by informing people how we are going to use it, who we may share it with, how long we will keep it.
- **Consent** — Whilst we have legitimate legal reasons for collecting and processing personalised data, we will ask for your consent for a range of activities and data processing so that we and you are able to evidence consent was freely given.
- **Data agreements** — We will have written arrangements with external organisations such as East Sussex County Council if they are processing data for us, such as EYFE. We will ensure that anyone processing data on our behalf will be compliant with the GDPR requirements.



- **Appointing a data protection officer** —Yve Puxty (Manager) will be the Designated Data Officer supported by the Trustees. Yve Puxty will be the person who takes the lead on data compliance within the pre-school and to ensure compliance with GDPR.
- **Breach notification** — We acknowledge our obligation to notify the Information Commissioners Office (ICO) of any data breach within 72 hours of becoming aware of the breach.
- **Penalties** — We acknowledge that failure to comply with GDPR obligations may result in heavy penalties for each data breach.

Netherfield Pre-school's Approach to Upholding GDPR Individual Rights

GDPR provides individual rights for all parties concerned with the creation, storage and sharing of data and Netherfield Pre-school fulfils our obligations under these rights as follows:

The Right to be Informed

Netherfield Pre-school is registered with Ofsted and the Local Authority and consequently, is required to collect and manage certain data, such as:

- Parent's/Carer's names, addresses, work details, names of family members living at the same address, telephone numbers, email addresses, bank details, date of birth and National Insurance numbers.
- We need to know children's' full names, addresses, date of birth and Birth Certificate number, plus other information relating to their health and well-being as contained in our registration packs and individual online profiles (Tapestry).
- For parents claiming the free nursery entitlement we are requested to provide this data to East Sussex County Council; this information is sent to the Local Authority via a secure electronic file transfer system.
- We are required to collect certain details of visitors to Netherfield Pre-school. We need to know visitor's names, telephone numbers, addresses and where appropriate company name. This is in respect of our Health and Safety and Safeguarding Policies.
- As an employer we are required to hold data on our employees; names, gender, addresses, email addresses, telephone numbers, date of birth, National Insurance number, payroll and tax, bank details. Personal home and work contact details, emergency contact details of next of kin. Contract data including details of role, reporting structure, job location, holiday entitlement, notice period, working hours, and amendment to contract letters. Probation, overtime, lateness, any leave, family leave, privacy notices and data processing consent records. Working time, absence, qualification and skills, training, loans, advancements and deductions from wages, court orders. Statutory pay, expenses records, pension, benefit schemes, leaver's report, exit interviews. Job offers - not accepted, employee photograph. Data on any reportable accident, death or injury in connection with work. Allergies, CVs of rejected applicants, CVs of applicants offered jobs but not accepted. References provided by third parties for job offers whether accepted or not, CVs of current employees, application forms of current employees, employment contracts. Disciplinary records, grievance records, capability / poor performance records, appraisal /supervision/



performance records, absence management records, training agreements, redundancy consultations, HMRC records. Identification records, details of right to work in UK including any work permit.

- Information is also required for Disclosure and Barring Service checks (DBS) and proof of eligibility to work in the UK. This information is sent via a secure file transfer system to our provider for the processing of DBS checks. DBS information includes;
 - Disclosure and Barring Service (DBS) checks pre-recruitment
 - Disclosures of criminal records during employment
 - DBS periodic updates

The Right of Access

At any point an individual can make a request relating to their data and we will need to provide a response (within 1 month). We can refuse a request, if we have a lawful obligation to retain data i.e. from Ofsted in relation to the EYFS, but we will inform the individual of the reasons for the rejection. The individual will have the right to complain to the ICO if they are not happy with the decision.

The Right to rectification

This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)). At any point an individual can make a verbal or written request for rectification of their data and we will need to provide a response (within 1 month). This right is for individuals to have inaccurate personal data rectified, or completed if it is incomplete. In certain circumstances we can refuse a request for rectification. Netherfield Pre-school will take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary.

The Right to Erasure or Deletion

You have the right to request the deletion of your data where there is no compelling reason for its continued use. However, Netherfield Pre-school has a legal duty to keep children's and parents' details for 3 years after leaving the setting. Staff records must be kept for 6 years after the member of staff leaves employment, before they can be erased. This data is archived securely and shredded after the legal retention period.

The Right to Restrict Processing

Parents, visitors and staff can object to Netherfield Pre-school processing their data. This means that records can be stored but must not be used in any way, for example reports or for communications. If the restriction does not enable us to perform our childcare service, we will consult with the requester to find an acceptable solution. If none can be found then the childcare service may be discontinued.



The Right to Data Portability

Netherfield Pre-school requires data to be transferred from one IT system to another; such as from us to the Local Authority, to other settings, to HMRC RTI portal, and to 'Tapestry' Online Learning Journal. These recipients use secure file transfer systems and have their own policies and procedures in place in relation to GDPR.

The Right to Object

Parents, visitors and staff can object to their data being used for certain activities like marketing or research.

The Right related to automated decision-making including profiling

Automated decisions and profiling are used in marketing based organisations. Netherfield Pre-school does not use or share personal data for such purposes.

Collecting Personal Data

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. The data needs to be processed so that Netherfield Pre-school can fulfil a contract with the individual, or the individual has asked Netherfield Pre-school to take specific steps before entering into a contract.
2. The data needs to be processed so that Netherfield Pre-school can comply with a legal / Ofsted obligation.
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
4. The data needs to be processed so that Netherfield Pre-school can carry out its official functions.
5. The data needs to be processed for the legitimate interests of Netherfield Pre-school or a third party (provided the individual's rights and freedoms are not overridden).
6. The individual (or their parent/carer when appropriate in the case of a registered child at Netherfield Pre-school) has freely given clear consent.

Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/ carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable them to provide services to us – for example, IT companies. When doing this, we will only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.



- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.

Subject Access Requests to Netherfield Pre-school - Adults

Individuals have a right to make a 'subject access request' to gain access to personal information that Netherfield Pre-school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or the criteria used to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter or email to:

Yve Puxty

Netherfield Pre-school

Darvel Down

Netherfield

Battle

East Sussex

TN33 9QF

Email. netherfieldpreschool@hotmail.co.uk

Subject Access Requests to Netherfield Pre-school - Children

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.



Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from our parents or carers will be considered without the express permission of the child.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

CCTV

We use CCTV in various locations around Netherfield Pre-school to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to Yve Puxty.

Photographs and Videos

As part of Netherfield Pre-school activities and as part of your child's learning profile, we may take photographs and record images of individuals and / or children. We will obtain written consent from parents and carers for



photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to the parent and carer. Authorised uses may include:

- Within Netherfield Pre-school on notice boards, pegs, drawers, observations, etc.
- Outside of Netherfield by external agencies such as a Netherfield Pre-school appointed photographer.
- Online on Netherfield Pre-school's website, 'Tapestry' online learning journal or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Storage of Paper or Digital Information/ Media

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- All paper copies of children's and staff records are kept in a locked office and locked filing cabinets in Netherfield Pre-school. Members of staff can have access to these files but information taken from the files about individual children is confidential and apart from archiving, these records remain on site at all times. These records are shredded after the retention period.
- Papers containing confidential personal data will not be left on office and playroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from Netherfield Pre-school office.
- Passwords will be used to access nursery computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals.
- Encryption software will be used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff who store personal information on their personal devices (phones) are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of Data

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.



Data Audit and Procedure

To ensure Netherfield Pre-school is complying with GDPR a full data audit will be conducted every 2 years to ensure that there is a valid reason to hold data, that permission to hold all data has been sought and that the risk of data breaches is minimised.

- Find and record all documents either paper and/or on computer that contain information identifying a person / child, whether shared or not.
- Print off one copy of the relevant document.
- Identify if (1) the document can be deleted (2) the document can be archived and for how long (3) the document is current. (4) the document needs updating.

During the Data Audit it is necessary to make sure that we have consent for every piece of data held –if there is no specific permission this must be gained if the data is to be kept.

Netherfield Pre-school Areas to be Audited

There are many areas within Netherfield Pre-school that contain both paper and digital data and these need to be assessed for validity, security and compliance:

- Tapestry assessment and learning journal software
- Accounting software
- Microsoft Office
- Microsoft Outlook for email
- Registration and 'All about Me' forms
- Children's files
- Records of allergies – in files and on board in kitchen
- Child Protection/Safeguarding information
- EYEE funding information
- Attendance records
- Staff files
- Contact file
- Information held in all rooms
- Information on hardware; computers, iPads, laptops external hard drives – portable devices should not be removed from the data controller premises unless encrypted, PCs need to be locked every time user leaves the desk
- Information stored in office desks or shelves must be secure if it holds personal data
- Information held in remote offices (or at home if portable device taken from controller premises) – access to these by people not entitled to view it, i.e. anyone in the household must be restricted by secure systems/processes.



Staff Responsibilities

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
 - Informing Netherfield Pre-school of any changes to their personal data, such as a change of address.
- Staff should contact the Yve Puxty in the following circumstances:
1. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure - if they have any concerns that this policy is not being followed.
 2. If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
 3. If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
 4. If there has been a data breach.
 5. Whenever they are engaging in a new activity that may affect the privacy rights of individuals – if they need help with any contracts or sharing personal data with third parties.

Data Breach - Procedure

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify Yve Puxty, who will:

- investigate the report and determine whether a breach has occurred. To decide, she will consider whether personal data has been accidentally or unlawfully: - lost - stolen -destroyed - altered - disclosed or made available where it should not have been – made available to unauthorised people.
- make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- assess the potential consequences, based on how serious they are, and how likely they are to happen.
- work out whether the breach must be reported to the ICO.
- document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, will do this via the 'report a breach' page of the ICO website within 72 hours.
- also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, she will promptly inform, in writing, all individuals whose personal data has been breached.
- notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- meet with the Trustees to review what happened and how it can be prevented from happening again.

**Data Retention – Timescales****Related to Children**

Type of Personal Data	Retention Period
Children's records including registers medication, accident books	3 years after child has left
Child protection and safeguarding records	Until the child is 24
Records of reportable injuries, death, disease or dangerous occurrence.	3 years after the record was made
Accident/medical records as specified by COSHH 4	40 years from the date of the last entry

Related to Employees

Type of employee personal Data	Details of employee personal Data	Data retention period	Business case/need for data retention	Method of data deletion
DATA THAT MAY BE ENTERED INTO COMPUTER SOFTWARE SPECIFIC FIELDS				
Recruitment data	Job offers - not accepted	6 months from the date of offer or rejection, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	A candidate may make a discrimination claim during or after the selection process. Information may therefore be required to defend a claim.	Automated system deletion 6 months after the date of offer or rejection, except if any claim is made within that time, or notification received of an ongoing dispute, in which case the claimant's data will be deleted on completion of the claim.
Contact / Personal data	Personal home and work contact details Emergency Contact details of next of kin Employee Photo	While employment continues and for 12 months from the date employment ceases, except if any claim is made within that time in which case the claimant's data will be held until completion of the claim.	To allow for contact to be made in the first year after employment ends to deal with any immediate issues arising.	Automated system deletion 12 months after termination date, except if any claim is made within that time, or notification received of an ongoing dispute, in which case the claimant's data will be held until completion of the claim.



General Employment Contract data	Contract data including details of role, reporting structure, job location, holiday entitlement, notice period, working hours, and amendment to contract letters Probation data Overtime and TOIL data Lateness data Annual leave data Family leave data Privacy notices and data processing consent records Working time data	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
Performance and Training data	Absence data Appraisal data Probation data Qualification and skills data Training data Employee of the month and Good Job data	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
Pay and Benefits data	Payroll and tax data Date of birth Gender Loan data Advancements and deductions from wages data Court Orders data Statutory Pay data Bank Account details Expenses records Pension data Benefit schemes data	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim still outstanding, in which case the claimant's data will be held until completion of the claim.	Statutory retention period under the Taxes Management Act 1970 of 6 years after the last day of the last complete tax year during which they worked.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim still outstanding in which case the claimant's data will be deleted on completion of the claim.



Leavers data (not covered elsewhere)	Leaver's report	6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
Health and Safety data	Data on any reportable accident, death or injury in connection with work Allergies data	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim. (Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) 40 years from the date of the last entry Requirement The Control of Substances Hazardous to Health Regulations 2002 (COSHH))	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.

DATA THAT MAY BE HELD BY NETHERFIELD PRE-SCHOOL AS CONTROLLER IN EMPLOYEE DOCUMENTS / FILE NOTES ON OUR COMPUTER SOFTWARE SYSTEM OR ELSEWHERE, INCLUDING ON PAPER

Recruitment documents	CVs of rejected applicants CVs of applicants offered jobs but not accepted References provided by third parties for job offers whether accepted or not	6 months from the date of offer or rejection, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	A candidate may make a discrimination claim during or after the selection process. Information may therefore be required to defend a claim.	Automated system deletion 6 months after the date of offer or rejection, except if any claim is made within that time, or notification received of an ongoing dispute, in which case the claimant's data will be deleted on completion of the claim.
-----------------------	--	---	---	--



General Employment Contract documents	CVs of current employees Application forms of current employees Employment Contracts Probation records	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
Performance and Training records	Disciplinary records Grievance records Capability / Poor Performance records Appraisal / Performance records Probation records Absence Management records Family Leave records Training agreements Qualification and skills documents, including professional certificates and driving licence copies Redundancy consultations	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
Pay and Benefits records	HMRC records Loan agreements Court Order records Statutory Pay records Bank Account details Expenses records Pension records Benefit schemes records	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim made within that time, in which case the claimant's data will be held until completion of the claim.	Statutory retention period under the Taxes Management Act 1970 of 6 years after the last day of the last complete tax year during which they worked.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim still outstanding in which case the claimant's data will be deleted on completion of the claim
Leavers records (not covered)	Exit interviews Redundancy records	6 years after the last day of the last complete tax year during which they worked, except if any	As there is the possibility that any documents relating to an employee could be	Automated system deletion 6 years after the last day of the last complete tax year



elsewhere)		claim is made within that time, in which case the claimant's data will be held until completion of the claim.	relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
Health and Safety records	Records of any reportable accident, death or injury in connection with work Allergies data	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
Immigration checks	Identification records Details of right to work in UK including any work permit	Whilst employment continues and for 2 years after the termination date of employment.	Legal obligation based on Home Office guidance issued under Immigration, Asylum and Nationality Act 2006, to retain copies of right to work documents during employment and for 2 years after they stop working for you.	Automated deletion two years after the last day of employment
Criminal convictions records	Disclosure and Barring Service (DBS) checks pre-recruitment Disclosures of criminal records during employment DBS periodic updates	1A. Pre-recruitment checks for job offers not accepted or withdrawn will be deleted 3 months after offer date, except if any claim is made within that time, or notification received of an ongoing dispute, in which case the claimant's data will be deleted on completion of the claim. 1B. Pre-recruitment checks for current employees will be deleted in accordance with the General Employment Contract Documents retention	1. Pre-recruitment checks or disclosures during employment need to be carried out or held if the employee is dealing with large amounts of sensitive data, or if otherwise necessary for the purposes of carrying out employment rights and obligations. These checks or disclosures may be a document relevant to any tribunal, County Court or High Court claim, and therefore to be retained for up to 6	Pre-recruitment checks for job offers not accepted or withdrawn - manual deletion 3 months after offer date, except if any claim is made within that time, or notification received of an ongoing dispute, in which case the claimant's data will be deleted on completion of the claim. Where DBS check is necessary for the purposes of carrying out employment



		period above. 2. Where DBS check or disclosure during employment is necessary for the purposes of carrying out employment rights and obligations, it will need to be kept during employment and will need to be regularly updated, and any update will replace the previous DBS check which should then be deleted. 3. On termination of employment, a current DBS check or disclosure during employment will be held for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	years after termination of employment. 2. Where replacement DBS checks are provided on a regular basis, the old check will be kept on the system whilst it is established whether any potential claim for which the DBS check may be relevant will be made in relation to that previous period.	rights and obligations an old DBS check will be deleted 12 months after storing of new updated DBS check unless any claim is still outstanding, in which case the claimant's data will be deleted upon completion of the claim. Where DBS check or disclosure during employment is necessary for the purposes of carrying out employment rights and obligations, a current DBS check or disclosure during employment will be automatically deleted 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.
File Notes	Any Data included in File Notes	While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.	As there is the possibility that any documents relating to an employee could be relevant to a tribunal, County Court or High Court claim, we are following current ICO guidance to keep employee files for 6 years following the end of employment.	Automated system deletion 6 years after the last day of the last complete tax year during which they worked, unless any claim is still outstanding in which case the claimant's data will be deleted on completion of the claim.



PRIVACY NOTICE (on notice board in hallway and welcome packs)

Netherfield Pre-School processes personal information about its children and is a 'data controller' for the purposes of Data Protection legislation. We collect information from you and may receive information about your child from their previous setting. If we do receive data from your child's previous setting, we will make you aware of this and remind you that you have the option of erasure if you wish.

We will only collect data that is absolutely necessary and will only use the data for the reason it is initially obtained, as stated below.

The categories of child level information that we collect, hold and share include:

- Personal information (such as name, age and address)
- Characteristics (such as ethnicity, language, nationality and country of birth)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Medical information
- Special educational needs information
- Digital images and video footage
- Photocopies of identification (i.e. birth certificates/passports)

Why we collect and use this information:

- to support children's learning to provide evidence of development
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to allow parents/children to access EYPP Funded Childcare
- to monitor and report on children's progress

The lawful basis on which we use this information:

We collect and use children's information and special category data under the lawful basis of "legal obligation", in line with **GDPR Articles 6(1)(c) and 9(2)(a)**:

"processing is necessary for compliance with a legal obligation to which the controller is subject" –

Article 6(1)(c)

"the data subject has given explicit consent to the processing of those personal data for one or more specified purposes" - **Article 9(2)(a)**

Collecting children's information

Whilst the majority of child level information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain child level information to us or if you have a choice in this.

Storing pupil data

If the child goes to another setting, any relevant data (such as assessment information and safeguarding information) will be passed directly to the next setting. A 'Transfer of Information' document will be completed by the new setting/school as proof of transfer.

Online data on Tapestry will be deleted or passed on to the child's next setting, and all data erased from the pre-school records.



If a child does not move to another setting, their personal data will be stored for one academic year – in the chance of them moving to another setting and the setting contacting us for relevant information - before being destroyed.

Some development and assessment data (such as Early Years Pupil Premium evaluations and cohort development data) will be stored for up to five academic years to ensure we can provide sufficient evidence to inspection bodies when required. This will contain the child's name and age/DOB only.

Paper data will be stored in a secure, locked location. Digital data will be kept on an encrypted memory stick.

Child records including medication forms, accident reports and any safeguarding information that is not passed onto the child's next setting will be kept for the required time frames (below) and stored in a secure, locked location. The required time from to keep safeguarding records is until the child is 24 years. The required time frame to keep medication and injury records is 20 years unless specified by COSHH which is 40 years.

Who we share children's information with

We routinely share children's information with:

- settings/schools that the children attend after leaving us
- our local authority (East Sussex County Council)
- the Department for Education (DfE)
- other professionals such as Health Visitors, Social Workers and such like the online learning journal database, Tapestry

Requesting access to your personal data

Under data protection legislation, parents and children have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Pre-School Manager, Yve Puxty on 01424 838714.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance.

Alternatively, you can contact the Information Commissioner's Office at

<https://ico.org.uk/concerns/>

Why we share children's information

We do not share information about our children without consent unless the law and our policies allow us to do so.

We share children's' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins the settings funding and educational attainment policy and monitoring.

Data collection requirements:



To find out more about the data collection requirements placed on us by the Department for Education (for example; via the early years census) goes to

<https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our children to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information about Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our children from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data?
- the purpose for which it is required
- the level and sensitivity of data requested and the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

Data Protection Officer: Yve Puxty – Manager



5.3 Information and Records Policies and Procedures - Comments and Complaints

Policy Statement

Netherfield pre-school aims to provide a safe, stimulating and caring environment where children and their families feel welcome and valued. We believe in working together with parents to ensure their children's needs are met. We welcome comments from parents about our provision and recognize parents are the prime educators and that comments, whether negative or positive, about our setting are made with the child's interest at heart. Positive comments are a good way for parents to let settings know their work is valued and appreciated, and give everyone concerned the chance to build on good practice which promotes children's development. Parents are encouraged to praise where appropriate.

Procedures

Netherfield Pre-school will ensure that:-

- We are aware that complaints are clear expression of dissatisfaction with the group, its personnel or its services.
- The procedure will deal with specific concerns including a risk to health or safety of any individual or improper conduct or unethical behaviour.
- Anyone may file a complaint including children, parents, carers, volunteers, paid workers, or other people outside the group.
- Making a complaint is as easy as possible.
- Complaints are treated seriously whether it is made in person, by telephone, or by e-mail.
- Complaints will be dealt with promptly, politely and respectfully.
- The group learns from complaints and uses them to improve its services.

How to make a complaint

Complaints can be made in person, by telephone or in writing. The complaint may be resolved straight away by talking to the manager or person in charge.

The manager or person in charge will provide a complaint record form. (sample attached)

The complaint form will be forwarded to the chairperson of the group for action.

Ofsted will be informed of a complaint made against the group. Contact Ofsted on **0300 123 4666** or Ofsted.gov.uk.

Everyone involved in the complaint will be expected to treat the information as confidential.



5.4 Information and Records Policies and Procedures - Complaints Record (sample)

By law (see page 39 of the *Statutory framework for the early years foundation stage* booklet), registered childcare providers must make parents aware of their complaints procedures, including how to make a complaint to Ofsted. To ensure it's clear to all, the procedure should ideally be in writing, and signed by a parent of each child. (Where a childcare provider is registered on the Childcare Register, their complaints procedure **must** be in writing.) All written complaints that relate to the childcare requirements **must** be recorded and investigated by the childcare provider, and they must notify the complainant of the outcome within 28 days. Records should be kept for at least 3 years and must be available to parents and to Ofsted.

If an allegation of serious harm or abuse is made against the childcare provider or anyone who lives or works with them, the childcare provider **must** notify Ofsted and their local authority's Children's Social Care department immediately. This is a legal requirement (see page 21/22 of the Statutory Framework).

This sample form can be photocopied, or you can make your own if you ensure it includes the necessary information.

Date of complaint:			
A: Source of complaint			
Parent (in writing, including email*)	☐	Staff member / Assistant	☐
Parent (in person)	☐	Anonymous	☐
Parent (phone call)	☐	Ofsted (include complaint number if known)	☐
		Other (please state)	☐
B: Nature of complaint (tick more than one if necessary)			
▫ Child Protection / Safeguarding	☐	▫ Behaviour management	☐
▫ Communication with parents	☐	▫ Suitability of childcare provider/ other adult	☐
▫ Premises / security / safety	☐	▫ Adult:child ratio/condition of registration	☐
▫ Equal opportunities	☐	▫ Furniture/equipment/toys/facilities	☐
▫ Special needs	☐	▫ Organisation/ meeting children's needs	☐
▫ Medication procedures	☐	▫ Documentation	☐
▫ Illnesses / injuries procedures	☐	▫ Learning and development / activities	☐
▫ Food and drink	☐	▫ Other	☐
▫ Smoking	☐		

**Details of the complaint:**

Note: If it is impossible to retain confidentiality in this record, you will also need to maintain a separate record which outlines the complaint without disclosing the identity of the complainant or any particular child (ren).

Please turn over

C: How the complaint was dealt with (tick more than one if necessary)

Internal investigation

☐

Investigation by Ofsted

☐

Investigation by other agencies (please specify)

☐**Details of any internal investigation:**

In the case of investigation by Ofsted, attach any outcomes letter / Ofsted correspondence

D: Actions and outcomes

Internal actions

☐

Other action taken by Ofsted

☐

Actions that were agreed with Ofsted

☐

No action

☐

Changes to conditions of registration

☐

Actions imposed or agreed with other agency

☐**Details of actions and outcomes:**Outcome notified to complainant: Yes ☐

Date:

Has a copy of this record been shared with parents? Yes ☐No ☐

Name of registered childminder:

Childminder's signature:

Date completed:



5.5 Information and Records Policies and Procedures - Admissions and settling In (transitions)

Policy Statement

At Netherfield Pre-school we want children and families to enjoy being involved. Children need to know that other adults care about them and will help them to play with the activities offered at our setting. Parents need to feel confident in the ability of the adults in our setting, that they are able to look after and encourage their children to benefit from time spent in our setting. Upset children cannot relax and enjoy the activities available. Children need to form strong friendship groups to help them through transitions.

Procedures

- Netherfield Pre-school welcomes all families from the area.
- In order for families to know this we publicize our services in local shops, community centres, schools and the local news publication.
- We provide information both verbally and in the form of a booklet for new families.
- We ensure that this information reflects that all families are welcome into our group.
- Regular newsletters are supplied throughout the year informing parents and carers of our current topics, helpful information, fundraising and general news.

When children are ready to start the Pre-school we will:-

- Encourage parents, with their child, to visit our setting on a number of occasions before their child is due to start attending alone.
- We will agree with the parents how we will introduce and settle their child into our setting, to ensure that the individual needs of the child are met.
- We will welcome parents at our sessions until they feel confident that their child has settled and no longer needs them to stay.
- We will reassure parents, who are anxious about their child, information about their child's activities and welfare while attending our session.
- We will introduce new starters in small numbers over a period of time to allow each child the time and support needed to settle.
- Each new starter will be allocated a key worker who will work with the parent and the child to ensure the settling in process is made as easy as possible.



5.6 Information and Records Policies and Procedures - Animals in the setting

Policy statement

Children learn about the natural world, its animals and other living creatures, as part of the Learning and Development Requirements of the Early Years Foundation Stage. This may include contact with animals, or other living creatures, either in the setting or on visits. We aim to ensure that this is in accordance with sensible hygiene and safety controls.

Procedures

Animals in the setting as pets

- We take account of the views of parents and children when selecting an animal or creature to keep as a pet in the setting.
- We carry out a risk assessment with a knowledgeable person accounting for any hygiene or safety risks posed by the animal or creature.
- We provide suitable housing for the animal or creature and ensure that it is cleaned out regularly and is kept safely.
- We ensure that the correct food is offered, at the right times.
- We make arrangements for weekend and holiday care for the animal or creature.
- We register with the local vet and take out appropriate pet care health insurance.
- We make sure all vaccinations and other regular health measures, such as de-worming, are up-to-date and recorded.
- Children are taught correct handling and care of the animal or creature and are supervised.
- Children wash their hands after handling the animal or creature and do not have contact with animal soil or soiled bedding.
- Staff wear disposable gloves when cleaning housing or handling soiled bedding.
- If animals or creatures are brought in by visitors to show the children, they are the responsibility of the owner.
- The owner carries out a risk assessment, detailing how the animal or creature is to be handled and how any safety or hygiene issues will be addressed.

Visits to farms

- Before a visit to a farm, a risk assessment is carried out – this may take account of safety factors listed in the farm's own risk assessment, which should be viewed.
- The outings procedure is followed.
- Children wash their hands after contact with animals.

Legal framework

- The Management of Health and Safety at Work Regulations (1999)

Further guidance

- Health and Safety Regulation....A Short Guide (HSE 2003)