Westfield Nursery Nursery
General Data Protection Regulation (GDPR) Policy

Vision

At Westfield Nursery we aim to deliver against our vision 'Inspired beginnings, outstanding futures'.

Background

The General Data Protection Regulation (GDPR) is a piece of legislation which determines how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data. 'Personal data' means information that can identify a living individual.

Rationale

The Nursery collects and uses personal information about staff, children, governors, parents/ carers, students and other individuals who come into contact. This policy sets out the way personal data is processed fairly and lawfully.

Personal information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Nursery complies with its statutory obligations.

The Nursery is a data controller and must therefore comply with the data protection principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The Nursery must be able to demonstrate compliance. Failure to comply with the principles exposes the Nursery to possible financial penalties.

Details of the Nursery's purpose for holding and processing data can be viewed in the privacy notice which can be found on the website.

Please note, in some instances due to statutory regulations, this policy does not apply e.g. staff grievances, allegations of abuse.

Statement of Intent

Westfield Nursery aims to:

- Process personal data in compliance with the General Data Protection Regulations
- Ensure that staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities under this policy
- Safeguard the data protection rights of those involved with the Nursery community
- Instil confidence in the Nursery's ability to process data in a fair and secure way

Scope

This Policy applies to the following:

- Personal data of all Nursery employees, governors, pupils, parents and carers, volunteers and any other person carrying out activities on behalf of the Nursery
- The processing of personal data, both in manual form and on computer

Data Protection Principles

GDPR sets out the key principles that all personal data must be processed in line with. Westfield Nursery School will thereby ensure that personal data will be the following:

- Processed fairly, lawfully and in a transparent manner

- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed
- Accurate and, where necessary, kept up to date
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

There are also stronger rights for individuals regarding their own data. These rights are to be informed about what data is held, why it is being processed and who it is shared with; to access their data; to rectification of the record; to erasure; to restrict processing; to object to processing; to not to be subject to automated decision-making including profiling.

Roles and Responsibilities
The Governing Body and the Headteacher are responsible for implementing good data protection practices and procedures within the Nursery and for the compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy. The requirements of this policy are also mandatory for any third party contracted to provide services to the Nursery.

The Data Protection Officer (DPO) will have responsibility for all issues relating to the processing of personal data. The DPO will comply with responsibilities under the GDPR and will deal with subject access requests for rectification and erasure, and data security breaches. All complaints about data processing will be dealt with in accordance with the Nursery's Complaints Policy. The Nursery's Data Protection Officer is the Headteacher.

Strategies
- Staff will receive training on the data protection requirements with specific relation to Nursery policy
- GDPR protocols and practice will form part of the induction process for new staff
- Privacy Notices for staff and stakeholders will be transparent
- The GDPR Policy and Privacy Notices will be available on the Nursery's website

Consent
Where the Nursery seeks consent for processing personal data, such as the use of photographs, it will ensure that appropriate signed consent is obtained. Consent forms will detail how consent can be withdrawn. For our young children, written consent will be required from the adult with parental responsibility.
We currently ask consent for
-Participation in visits to Beecroft Community Centre/ Beecroft School
-Using the internet in school under supervision
-Photos for display in class (display/ learning journey)

-Photos/videos for school publications (newsletters/ brochure)
-Photos/videos for school website
-Photos/videos for school productions (e.g. Christmas/ end of year etc.)
-Class photos
-Photos in local press
-Class list with first names only (Christmas cards/ parties)

Location of Personal Information and Data
Hard copy data, records, and personal information are stored out of sight and in locked cupboards when not in use or unattended. The only exception to this is medical information that may require visibility or immediate access during the Nursery day and is necessary for the well-being of the person involved.

Sharing Data with Third Parties and Data Processing on Behalf of the Nursery
Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so e.g. local authorities, Ofsted or the Department of Education or Health. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the Nursery. The Nursery will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Data may be shared with the following:
- Education Establishments – Data will be shared to allow a smooth transition for pupils moving to another setting
- Health Authorities - As obliged under health legislation, the Nursery may pass on information regarding the health of children in the Nursery to monitor and avoid the spread of contagious diseases in the interest of public health.
- Police and Courts - If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- Social workers and support agencies - To protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- Educational division - Nurseries may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education

Subject Access Requests
Requests for access to personal data- Subject Access Requests (SARs) will be processed by the DPO. Those making a SAR will be charged a fee in accordance with regulations. Records of all requests will be maintained.

The Nursery will comply with the statutory time limits for effecting disclosure in response to a SAR. The statutory time limit is one calendar month of receipt of the request (barring school holiday times).

Data Protection Breaches
Breaches of personal or sensitive data will be notified within 72 hours to the individual(s) concerned and the Information Commissioners Office (ICO).

Disposal of Personal Data
See Record Retention and Disposal Policy

Guidelines for Staff:

- All passwords used to access computers, memory sticks or systems where personal data is stored must use a mixture of lower case letters, upper case letters, symbols and numbers in their passwords
- Nursery computers should be locked or shut down when unattended and at the end of the Nursery day
- Only transport electronic information from Nursery on a secure computing device i.e. password protected laptops and memory sticks
- Use pseudonyms and anonymise personal data where possible
- Ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'
- Avoid taking paper-based documentation out of Nursery wherever possible. If paper-based documentation is taken out of Nursery, then please ensure that it is kept secure e.g. lockable drawer at home or in a sealed envelope which indicates a return address if misplaced. Return it to Nursery as soon as possible
- When transporting paper-based documentation, make sure that it is locked during transit e.g. in the locked boot of a car. Never leave documentation in vehicles overnight
- Lock documentation containing personal information away at night and when not being used during the daytime
- Shred documentation containing personal information and never put paper-based documents containing personal information into recycling bins
- Collect paper copies of printouts containing personal information from printers/photocopies straight away
- Avoid e-mailing documents to personal e-mail addresses
- Never store work related documents on a shared home computer and never let Nursery computers/laptops be used by others e.g. son's/daughter's homework use
- Only print off documents containing personal data if necessary
- Report any loss of paper-based information or portable computer devices to the DPO immediately
- Personal passwords, where the accessing of personal data is possible, must not be shared with others. Passwords of staff leaving the Nursery should be changed/removed in a timely manner
- The personal details of others, at social events or in public places, must not be discussed. Take care if reading documentation containing personal information on public transport or leaving personal information unattended in a public place e.g. meeting, course
- Only copy necessary recipients into e-mail correspondence and only post necessary information when sending information via the postal service
- Always ask the DPO if you are unsure about storage/transportation or sharing of information containing personal information

Visitors

Visitors will be made aware of GDPR requirements and visitors, when signing in, acknowledge that they won't share or publicise anything from their visit without first gaining explicit consent from the nursery.

Conclusion

The implementation of this policy, along with the Record Retention & Disposal Policy, the Data Breach Procedures Policy and Privacy Notice will demonstrate the Nursery's desire to comply with GDPR.

Policy reviewed March 2022

Westfield Nursery School

Record Retention & Disposal Policy

Vision

At Westfield Nursery we aim to deliver against our vision ‘Inspired beginnings; outstanding futures’.

Introduction

Westfield Nursery creates and holds a wide range of recorded information. Records need to be properly retained to enable Nursery to meet its educational needs, legal requirements, to evidence events or agreements in the event of allegations or disputes and to ensure that any records of historic value are preserved.

The untimely destruction of records could affect:

- the conduct of Nursery’s business
- the ability of Nursery to defend or instigate legal actions
- Nursery’s ability to comply with statutory obligations
- Nursery’s reputation

Conversely, the permanent retention of records is undesirable, and disposal is necessary to free up storage space, reduce administrative burden and to ensure that Nursery does not unlawfully retain records for longer than necessary (particularly those containing personal data).

This policy supports Nursery in demonstrating public accountability through the proper retention of records and by demonstrating that disposal decisions are taken with proper authority and in accordance with due process.

Purpose

The purpose of this policy is to set out the length of time that Nursery’s records should be retained and the processes for disposing of records at the end of the retention period.

Scope

The policy covers the records listed below, irrespective of the media on which they are created or held including- paper and electronic files and can include photographs, pupil records, minutes of meetings, submissions from external parties, contracts and invoices, registers, legal advice, file notes, financial accounts, employee information and Nursery’s publications.

Should you become aware of any records missing from the list, please notify the head teacher so that they may be added at the next opportunity.

Application

The policy applies equally to full time and part time employees on a substantive or fixed-term contract and to associated persons who work for Nursery such as supply staff, contractors and others employed under a contract of service.

Minimum Retention Period
A recommended minimum retention period is provided for each category of record in listed below. The retention period applies to all records within that category.

Disposition
The head teacher and governing body are responsible for ensuring that the retention periods are reviewed annually. The senior leadership team are required to determine whether any retention periods applying to records have expired. Once the retention period has expired, the record must be reviewed and a 'disposition action' agreed upon.

A 'disposition action' is either- the destruction of the record or the retention of the record for a further period within Nursery. No destruction of a record should take place without assurance that:
- the record is no longer required by any part of the Nursery
- no litigation or investigation is current or pending which affects the record

Destruction of Paper Records
Destruction should be carried out in a way that preserves the confidentiality of the record. Non-confidential records i.e. records that are clearly in the 'public domain' can be placed in ordinary rubbish bins or recycling bins.

Confidential records should be shredded. All copies including security copies, preservation copies and backup copies should be destroyed at the same time in the same manner.

Destruction of Electronic Records
All electronic records will need to be either physically destroyed or wiped.

Any queries about this policy or about records management within Nursery should be directed to the head teacher.

Conclusion
The implementation of this policy, along with the GDPR Policy, Data Breach Procedures Policy and Privacy Notice will demonstrate the Nursery's desire to comply with GDPR.

Policy reviewed November 2021
Policy to be reviewed November 2022

Westfield Nursery School
Data Retention Schedule

We follow the Central Bedfordshire guidelines on data record retention

RETENTION OF RECORDS GUIDANCE

Children's Records	Retention Period	Legislation
Children's records including registers, medication, parental permission forms, record books, contractual documentation, complaints book, local authority data for funded places and accident record books pertaining to children	Standard cases – recommended: 6 years after the child has left the setting	Early Years Foundation Stage 2017 Childcare Act 2006
Special circumstances: Serious complaint Child protection issues A child is badly injured A child is on regular medication A child has severe allergies A child has a serious illness	Recommended until the child reaches the age of 25. Seek legal advice about making and retaining copies, particularly if you are required to provide information to a third party	Limitation Act 1980 Normal limitation rules (which mean that an individual can claim for negligently caused personal injury up to 3 years after, or deliberately caused personal injury up to 6 years after the event) are postponed until a child reaches 18 years old.
Records of any reportable death, injury, disease or dangerous occurrence, accident/incident records and risk assessments specific to a child	Recommended that records are kept until the child reaches 25 years of age	The reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995
Other records containing personal information or images of children and families: Photographs/videos Websites Social media posts Texts Emails Apps Cloud storage	Keep photographic/video/audio-visual permissions given by parents on behalf of children for 21 years and 6 months Ensure written parental permission is in place to take and post photos and videos online Ensure data is stored in accordance with the data protection/confidentiality policy	ICO – Registration as a Data Controller GDPR 2018
Visitor's book	As a minimum, must be kept between inspection periods Seek legal advice in special circumstances (see above)	Early Years Foundation Stage 2017
Ofsted Reports	As a minimum, must be kept between inspection periods. Keep for reference as evidence of compliance and good practice	Early Years Foundation Stage 2017
Risk assessments	Standard cases – minimum 3 years from date recorded Special circumstances may need to be kept for longer (see above)	
Personnel Records	**Retention Period**	**Legislation**
Personnel files and training records (including application form, work history, references, supervision, 1:1s, appraisals, performance reviews, qualifications,	6 years after employment ceases	Chartered Institute of Personnel and Development Ofsted

disciplinary records, working time records and training records)		
CVs, application forms and interview notes (for unsuccessful candidates)	6 months to 1 year	Chartered Institute of Personnel and Development
DBS check/disclosure information Essential details to be recorded from the original DBS certificate, i.e. name, date of birth, reference number, date of issue	By law, the only details that can be kept for longer than 6 months are the date of the check, reference number and the result Recommended these details are kept for 6 years	DBS Code of Practice The following basic information should be retained after the certificate is destroyed: the date of issue; the name of the subject; the type of disclosure; the position for which the disclosure was requested; the unique reference number; and the details of the recruitment decision taken
Safeguarding – adult records	Retirement if concerns relating to potential abuse/behaviour unsuitable	Working together to safeguard children – LSCB
Wages/salary records (including overtime, bonuses and expenses)	6 years after the end of the tax year to which the records relate	Taxes and management Act 1970
Statutory Maternity Pay (SMP), adoption and paternity pay records	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay Regulations 1986
Statutory Sick Pay (SSP) records	3 years after the end of the tax year to which the records relate	The Statutory Sick Pay Regulations 1982
Income Tax and National Insurance returns/records	At least 3 years after the end of the tax year to which they relate	The Income Tax (Employments) Regulations 1993
Redundancy details calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	Chartered Institute of Personnel and Development
Health and Safety	**Retention Period**	**Legislation**
Staff accident records (for organisations with 10 or more employees)	3 years after the date the record was made (there are separate rules for the recording of accidents involving hazardous substance)	Social Security (Claims and Payments) Regulations 1979
Records of any reportable death, injury, disease or dangerous occurrence	3 years after the date on which the record was made	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)
Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 (COSHH)
Financial	**Retention Period**	**Legislation**
Accounting records Copy of self-assessment forms and supporting records of income and expenditure, including: Bank statements Receipts Invoices	Must be retained for at least 6 years (or at least 3 years in the case of charitable companies); where Gift Aid payments are received records will need to be maintained for 6 years with	Section 386 of the Companies Act 2006 Charities Act 2011

Cash book Gift Aid records Accounts book/records	details of any substantial donors and to identify 'tainted charity donations' in accordance with HMRC guidance	
Administration Records	**Retention Period**	**Legislation**
Public Liability Insurance Insurance records	For as long as possible e.g. 40 years from date of issue Recommended that complete records of all insurance policies taken out are kept Seek legal advice is a special circumstance (see above)	The employers' Liability Regulations 1998 Health and Safety Executive
Minutes/minute books	10 years from the date of the meeting for companies	Companies Act 2006
	6 years from the date of the meeting for Charitable Incorporated Organisations	The Charitable Incorporated Organisations Regulations 2012
	Permanently	Chartered Institute of Personnel and Development
Data Protection Audit	**Reviewed and updated annually**	

Policy reviewed November 2021
Policy to be reviewed November 2022

Westfield Nursery School
Data Breech Procedures Policy

Vision
At Westfield Nursery we aim to deliver against our vision ‘Inspired beginnings; outstanding futures’.

Rationale
At Westfield Nursery we understand the importance of taking measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

Data Breaches
A data security breach can happen for several reasons:
- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

Breach Management Plan
Our plan has four steps:
1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

Containment and Recovery
Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This may involve input from specialists e.g. IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:

At Westfield Nursery, generally the DPO will take the lead on investigating the breach and ensure they have the appropriate resources. They will
-establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, finding a lost piece of equipment or simply changing the access codes at the front door.
-establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back-up systems to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
-where appropriate, inform the police.

Assessing the Risks
Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. For example, where a laptop is irreparably damaged, but its files were backed up and can be recovered, albeit at some cost to the Nursery. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of pupil/ parent data, which may be used to commit identity fraud. The DPO must assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The DPO will consider:
-What type of data is involved?
-How sensitive is it?
-If data has been lost or stolen, are there any protections in place such as encryption?
-What has happened to the data?
-What the data could tell a third party about the individual?
-How many individuals' personal data are affected by the breach?
-Who are the individuals whose data has been breached?
-What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
-Are there wider consequences to consider such as a risk to public health or loss of public confidence?
-If individuals' bank details have been lost, contact the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification of Breaches
Notification will have a clear purpose (for example, to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints). Serious breaches will be reported to the Information Commissioners Office (ICO).

The DPO will consider:
-Any legal or contractual requirements
-Whether notification will help meet security obligations
-Whether notification will help the individual
-Whether to inform the ICO (If many people are affected, or there are very serious consequences, they will inform the ICO)
-How notification can be made appropriate for groups of individuals
-The dangers of 'over notifying'
-Who to notify, what to tell them and how to communicate the message

The notification should include a description of how and when the breach occurred and what data was involved; as well as details of what has already done to respond to the risks posed by the breach.

When notifying individuals, the DPO will give specific and clear advice on the steps they can take to protect themselves and what they are willing to do to help. They will be given details of how they can contact the DPO for further information or to ask questions about what has occurred.

When notifying the ICO the DPO will include details of the security measures in place such as encryption and, where appropriate, details of the security procedures in place at the time the breach occurred. The ICO should be informed if the media is aware of the breach.

(When informing the media, it is useful to inform them whether you have contacted the ICO and what action is being taken.)

Evaluation and Response

The governors will investigate the causes of the breach but also the effectiveness of the DPO's response to it. Existing procedures may need to be reviewed and improved.

The DPO needs to:

-Know what personal data is held and where and how it is stored

-Establish where the biggest risks lie

-Assess risks which will arise when sharing with or disclosing to others

-Identify weak points in existing security measures such as the use of portable storage devices

-Monitor staff awareness of security issues and fill any gaps through training or tailored advice

Conclusion

The implementation of this policy, along with the GDPR Policy, Record Retention & Disposal Policy and Privacy Notice will demonstrate the Nursery's desire to comply with GDPR.

Policy reviewed November 2021

Policy to be reviewed November 2022