Westfield Nursery School

General Data Protection Regulation (GDPR) Policy

Contents:

Date plan last reviewed: **May 2026**

Signed by:

_____ **Headteacher** **Date:** _____

_____ **Chair of governors** **Date:** _____

May 2026
-Updated legal framework
-Added reference to Data Use and Access Act (DUAA) June 2025
-Named Data Protection Officer
-Updated Subject Access Request information (inline with DUAA June 2025)
-Made clearer difference between school and external DPO role
-Added reference to strong, unique passwords & password changes when compromise is suspected

Vision and Statement of Intent

1. Legal Framework
2. Scope
3. Data Protection Principles
4. Applicable Data
5. Roles and Responsibilities
6. Lawful Processing
7. Consent
8. Strategies
9. Location of Personal Information and Data
10. Sharing with Third Parties & Data Processing on Behalf of the Nursery
11. The Right to be Informed
12. The Right to Access: Subject Access Requests
13. The Right to Rectification
14. The Right to Erasure
15. The Right to Restrict Processing
16. The Right to Data Portability
17. The Right to Object
18. Privacy by Design and Privacy Impact Assessments
19. Publication of Information
20. Photography
21. Data Security
22. Data Protection Breaches
23. Data Retention
24. DBS Data
25. Policy Review

Vision and Statement of Intent

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

As a data controller Westfield Nursery School is required to keep and process certain information about staff, children, governors, parents or carers, pupils, volunteers and other individuals who come into contact. This policy sets out the way personal data is processed fairly and lawfully in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

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. The regulation has applied to all settings from May 2018.

‘Personal data’ means information that can identify a living individual. Personal information is gathered to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure the Nursery complies with its statutory obligations, 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. The Nursery may be required to share personal information about its staff or pupils with other organisations, including the Local Authority, other schools and educational bodies, and social services.

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.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Nursery complies with the following core principles of the GDPR. Please note, in some instances due to statutory regulations, this policy does not apply e.g. staff grievances, allegations of abuse.

Westfield Nursery aims to:

- Process personal data in compliance with the General Data Protection Regulations
- Ensure 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

Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (GDPR) and Data Protection Act 2018
- The Freedom of Information Act 2000
- Data (Use and Access) Act (DUAA) June 2025

This policy will be implemented in conjunction with the following other Nursery policies:

- Acceptable Use Policy
- Safeguarding and Child Protection Policy

Scope

This policy applies to the following:

- Personal data of all Nursery staff, 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 electronically

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

Applicable Data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The GDPR applies to both automated personal data and to manual filing systems.

Sensitive Personal Data is referred to in the GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Roles and Responsibilities

Westfield Nursery School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.
The Nursery will provide comprehensive, clear and a transparent privacy policy.

Who is responsible for making sure data is processed securely in a Nursery?
Everyone in Nursery is responsible for protecting personal data. There are some key roles and responsibilities for data protection compliance.

Data Controller
The Nursery is the data controller. This means it's responsible under the Data Protection Act 2018 for protecting data in every situation where it decides:

- whose information to collect
- what types of data it needs
- why it needs it
- whether the information can be shared with a third party
- when and where data subjects' rights apply
- for how long to keep the data

Data Protection Officer (DPO) Internal
The internal data protection officer is responsible for:

- advising Nursery staff about their data obligations
- monitoring compliance
- conducting regular data audits (data impact assessments)
- developing and updating data protection policies and procedures
- monitoring who in the Nursery has access to personal data
- advising when data protection impact assessments are needed
- answering data protection enquiries from staff, parents/ carers and pupils
- making sure privacy notices are regularly reviewed and updated
- supporting and advising staff who have data protection queries
- communicating with the Information Commissioner's Office (ICO)
- reporting to the governing board about data protection
- advising the governing board on data protection risks
- advising on and co-ordinating responses to information rights requests
- making sure all assets containing personal data are appropriately managed and secure

The data protection officer should know about:

- data protection
- UK GDPR
- the way the Nursery operates
- the technology and systems the Nursery uses
- cyber security

Data Protection Officer (DPO) External
The internal data protection officer is responsible for:

- advising Nursery staff and in particular the internal DPO about their data obligations
- monitoring compliance
- support audits and review of these
- provide guidance
- answering data protection enquiries from staff, parents/ carers and pupils

The Nursery uses School Consulting Ltd, an External DPO service (advisory). The DPO will report to the headteacher. The DPO will operate independently and will not be dismissed or penalised for performing their task. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations. All complaints about data processing will be dealt with in accordance with the Nursery's Complaints Policy.

Governors
The responsibility and accountability for compliance sits with governors.
Governors check that the Nursery:

- monitors their data protection performance

- supports the data protection officer
- has good network security infrastructure to keep personal data protected
  has a business continuity plan in place that includes cyber security

Senior Leaders
Senior leaders are accountable for:
- deciding how the Nursery uses technology and maintains its security
- deciding what data is shared and how
- setting Nursery policies for the use of data and technology
- understanding what UK GDPR and the Data Protection Act covers and getting advice from the data protection officer, as appropriate
- assuring governors that the Nursery has the right policies and procedures in place
- making sure any contracts with third-party data processors cover the relevant areas of data protection
- making sure staff receive annual training on data protection, including specific Nursery processes such as personal data breach reporting processes and the escalation of information rights requests

Staff
All staff should be aware of what:
- personal data is
- 'processing' means
- their duties are in handling personal information
- the processes are for using personal information
- is permitted usage of that data
- the risks are if data gets into the wrong hands
- their responsibilities are when recognising and responding to a personal data breach
- the process is for recognising and escalating information rights requests

This includes:
- teaching staff
- first-aiders
- governors
- volunteers

There are extra requirements for any staff in Nursery who:
- create and store data
- enter data into applications or software
- decide if and when they'll process certain data
- handle paper documents

Staff who collect, store or view personal data are responsible for:
- making sure they have a legitimate need to process the data
- checking that any data they store is needed to carry out necessary tasks
- identifying any risks
- understanding the governance arrangements that oversee the management of risks

Lawful Processing
The legal basis for processing data will be identified and documented prior to data being processed. Under GDPR, data will be lawfully processed under the following conditions:
- The consent of the data subject has been obtained
- Processing is necessary for:

— Compliance with a legal obligation
— The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
— For the performance of a contract with the data subject or to take steps to enter into a contract
— Protecting the vital interests of a data subject or another person
— For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:

— Carrying out obligations under employment, social security or social protection law, or a collective agreement
— Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
— The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
— Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
— The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

Consent
Where the Nursery seeks consent for processing personal data, such as the use of photographs, it will ensure appropriate signed consent is obtained. For our young children, written consent will be required from the adult with parental responsibility. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given. The Nursery ensures consent mechanisms meet the standards of the GDPR. Consent can be withdrawn by the individual at any time.

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

Location of Personal Information and Data
Hard copy data, records, and personal information are stored out of sight and in 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 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

The Right to be Informed
The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear language, which is concise, easily accessible and free of charge.

The Right to Access: Subject Access Requests
Individuals have the right to obtain confirmation that their data is being processed. We may get subject access requests from:
- a parent/ carer wishing to see what data you hold about themselves or their child
- staff
- former staff or families
- a solicitor on behalf of a staff or families
- a governor

Before we respond to a subject access request raised by a parent/ carer about a child, we check if:
- the requester has parental responsibility for the child
- releasing the information to an absent parent/ carer would cause the child distress or result in safeguarding concerns

We consider the impact releasing the data would have on the child and their well-being before we respond.

We will not provide a pupil's educational record to a parent/ carer if there is a court order in place that limits the exercise of their parental responsibility.

Most of the personal data we hold about a pupil will form part of their educational record. For maintained Nurseries, a request for an educational record is different from a subject access request.

Requests for access to personal data (Subject Access Requests) (SARs) will be processed by the Data Protection Officer. Records of all requests will be maintained.

Handling Subject Access Requests
1. Time limit: We will respond to a SAR within one calendar month from the date the request is received, or from when any required information (e.g. identity verification or clarification of scope) is provided.
2. "Stop-the-clock" / pause: If we need more information from the requester (for example, to confirm their identity, or to clarify exactly what data they want), we may pause the time limit until we receive that. We will notify the requester as soon as possible the clock is paused, what information we need, and set a reasonable deadline for receiving that information.
3. Extension for complexity: If the request is complex or the requester has made multiple concurrent requests, we may extend the deadline by up to two further months, making a total of up to three calendar months. This extension will be communicated to the requester within the first month, with reasons.
4. Searches must be reasonable & proportionate: We will search for the information in ways that are reasonable and proportionate, not necessarily exhaustively, considering relevance, resources, and the type/volume of data we hold.
5. Record-keeping: We will document all steps: when request received, when identity was confirmed, when clarification was asked for (if applicable), reasons for any extension, and decision on the scope of search. And maintain our SAR log.

The Right to Rectification
Individuals are entitled to have any inaccurate or incomplete personal data rectified.
Where the personal data in question has been disclosed to third parties, the Nursery will inform them of the rectification where possible. Where appropriate, the Nursery will inform the individual about the third parties the data has been disclosed to. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, the Nursery will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure
Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

The Nursery has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- The exercise or defence of legal claims

The Right to Restrict Processing
Individuals have the right to block or suppress the Nursery's processing of personal data. In the event processing is restricted, the Nursery will store the personal data, but not further process it, guaranteeing just enough information about the individual has been retained to ensure the restriction is respected in future. The Nursery will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Nursery has verified the accuracy of the data
- Where an individual has objected to the processing and the Nursery is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Nursery no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the Nursery will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. The Nursery will inform individuals when a restriction on processing has been lifted.

The Right to Data Portability
Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The Nursery will provide the information free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

Westfield Nursery School is not required to adopt or maintain processing systems which are technically compatible with other organisations. In the event that the personal data concerns more than one individual, the Nursery will consider whether providing the information would prejudice the rights of any other individual. The Nursery will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request. Where no action is being taken in response to a request, the Nursery will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Object

The Nursery will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring it is presented clearly and separately from any other information. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation
- The Nursery will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Nursery can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

Privacy by Design and Privacy Impact Assessments

The Nursery will act in accordance with GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Nursery has considered and integrated data protection into processing activities.

Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the Nursery's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the Nursery to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Westfield Nursery Nursery's reputation which might otherwise occur. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling

The Nursery will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the Nursery will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Publication of Information

Westfield Nursery School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures

- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

Westfield Nursery School will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the Nursery website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

Photography

The Nursery understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The Nursery will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

Data Security

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Lock documentation containing personal information away at night and when not being used during the daytime e.g. Pupil Provision Maps
- 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 immediately
- Only print off documents containing personal data if necessary
- Avoid taking paper-based documentation out of Nursery wherever possible. If paper-based documentation is taken out of Nursery, then please ensure 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 it is locked during transit e.g. in the locked boot of a car. Never leave documentation in vehicles overnight
- Ensure 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'
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- All passwords should be strong, unique passwords and changed every three to six months or when compromise is suspected
- 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
- 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
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Staff and governors will not use their personal laptops or computers for Nursery purposes.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Avoid e-mailing documents to personal e-mail addresses

- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Only copy necessary recipients into e-mail correspondence and only post necessary information when sending information via the postal service
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Nursery premises accepts full responsibility for the security of the data.
- Take care if reading documentation containing personal information on public transport or leaving personal information unattended in a public place e.g. meeting, course Report any loss of paper-based information or portable computer devices to the Data Protection Officer/Headteacher immediately
- The personal details of others, at social events or in public places, must not be discussed.
- Anonymise personal data where required
- Always ask the Data Protection Officer/Headteacher if you are unsure about storage/transportation or sharing of information containing personal information

Before sharing data, all staff members will ensure:

- They are allowed to share it
- That adequate security is in place to protect it
- Who will receive the data has been outlined in a privacy notice

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Nursery containing sensitive information are supervised at all times. The physical security of the Nursery's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Westfield Nursery School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action. The Nursery business manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Data Protection Breaches
See Data Breach Policy

Data Retention
See Data Retention & Disposal Policy

Disposal of Personal Data
See Record Retention and Disposal Policy

DBS Data
All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Policy Review
This policy is reviewed every two years by the headteacher, SBM and DPO.
The next scheduled review date for this policy is May 2028.

Westfield Nursery School

Records Management Policy

Date policy last reviewed: _____

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

May 2026
-Added reference to Data Use and Access Act (DUAA) June 2025
-Changed to DfE Retention Schedule February 2026
-Removed reference to Information Records Management Society (IRMS) (2019), 'Information Management Toolkit for Nurseries' DfE (2023) 'Data protection in Nurseries' & DfE (2018) 'Data protection: a toolkit for Nurseries' as adopting latest DfE scheme

Contents:

Statement of Intent and Vision

1. Legal Framework
2. Roles and Responsibilities
3. Scope
4. Management of Records
5. Destruction of Records
6. Identifying Information
7. Information Audit
8. Monitoring and Review

Vision & Statement of Intent
At Westfield Nursery School we aim to deliver against our vision 'Inspired beginnings, outstanding future.'

Westfield Nursery School creates and holds a wide range of recorded information to enable us to meet educational needs, legal requirements, to evidence events or agreements and in the event of allegations or disputes and to ensure any records of historic value are preserved. We are committed to maintaining the confidentiality of its information and ensuring all records within the Nursery are only accessible to the appropriate individuals. In line with the requirements of the UK GDPR. The Nursery also has a responsibility to ensure all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended. The Nursery has created this policy to outline how records are stored, accessed, monitored, retained and disposed of to meet the Nursery's statutory requirements.

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 and the 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. This document complies with the requirements set out in the UK GDPR and Data Protection Act 2018 and the Data Use and Access Act (DUAA) June 2025

Legal Framework
This policy has due regard to legislation including, but not limited to, the following:
- UK General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- Data Protection Act 2018
- Data Use and Access Act (DUAA) June 2025

This policy also has due regard to the following guidance:
- ICO (2023) 'How do we document our processing activities?
- ICO (2023) 'Controllers checklist'
- DfE (2026) 'Data Retention Schedule'

This policy will be implemented in accordance with the following Nursery policies and procedures:
- General Data Protection Policy
- Acceptable Use Policy

Roles and Responsibilities
The whole Nursery has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

The headteacher will hold the overall responsibility for this policy and for ensuring it is implemented correctly and will be responsible for:
- The management of records at the Nursery
- Promoting compliance with this policy and reviewing the policy every two years
- Ensuring all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of safely and correctly

All staff members will be responsible for ensuring any records they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

The policy applies equally to full time and part time staff 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.

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.

The Head teacher and governing body are responsible for ensuring the retention periods are reviewed annually. The senior leadership team are required to determine whether any retention periods applying to records have expired. No destruction of a record should take place without assurance the record is no longer required by any part of the Nursery, and no litigation or investigation is current or pending which affects the record.

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

Management of Records
All records will be dealt with in line with the Department for Education Retention of Records advice.
https://www.gov.uk/government/publications/retention-schedule-for-data-processed-by-dfe/dfe-retention-schedule

Destruction of Records
Destruction should be carried out in a way that preserves the confidentiality of the record. Non-confidential records i.e. records 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. All electronic records will need to be either physically destroyed or wiped. Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable.

Identifying information
Under the UK GDPR, all individuals have the right to data minimisation and data protection by design and default – as the data controller, the Nursery ensures appropriate measures are in place for individuals to exercise this right.

Information audit
The Nursery conducts information audits on an annual basis against all information held by the Nursery to evaluate the information the Nursery is holding, receiving and using, and to ensure this is correctly managed in accordance with the UK GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Knowledge
- Apps and portals

The information audit may be completed in a number of ways, including, but not limited to: interviews with staff members with key responsibilities – to identify information and information flows, etc.

The DPO is responsible for completing the information audit. The information audit will include the following:

- The Nursery's data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

Once it has been confirmed that the information is accurate, the DPO will record all details on the Nursery's Data Asset Register managed by the SBM.

Monitoring and review

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. This policy will be reviewed every two years by the Headteacher– the next scheduled review date for this policy is May 2028. Any changes made to this policy will be communicated to all members of staff and the governing board.

Westfield Nursery School

Data Protection Policy and Data Breach Response Plan

Date policy last reviewed: May 2026

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Last updated: May 2026

May 2026 New policy as advised by DPO

Content

Vision & Statement of Intent

1. Data Protection Policy and Data Breach Response Plan
2. Introduction
3. What is a personal data breach?
4. Understanding the risk to the rights and freedoms of individuals
5. Timescales for reporting a breach
6. Response plan
7. Record Keeping
8. Nursery Holidays
9. How do we protect our data?
10. Contact for IT support
11. Monitoring and Review

Vision & Statement of Intent

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

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.

1. **Data Protection Policy and Data Breach Response Plan**

This is an internal policy which works alongside Nursery GDPR logs and procedures (see main GDPR folder). It is to be read in conjunction with the Nursery Privacy Notice (website) and Privacy Notice for Staff, Governors and Volunteers (internal policy). An Online Safety Policy is followed by the Nursery to ensure all stakeholders, including staff, pupils and parents are abiding by the acceptable use standards.

2. **Introduction**

Westfield Nursery School has implemented appropriate technical and organisational policies, procedures and measures to avoid data security breaches. However, in the event that a data security breach happens, we recognise that is important that the Nursery is able to detect it and react swiftly and robustly in order to mitigate any risks to data subjects and to comply with our obligations under the General Data Protection Regulation ('GDPR').

This Data Breach Response Plan sets out how we will respond to any suspected or actual data breaches and should be read alongside Nursery GDPR policy and procedure.

The GDPR requires the Nursery to report 'notifiable breaches' without undue delay and, where feasible, not later than 72 hours after having become aware of it. Notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, which is a subjective measure determined jointly by the Data Breach Response Team (see 5.7). In the event that a report is not made within 72 hours, the Nursery is required to provide the reasons for the delay in reporting it to the ICO.

If there is deemed to be a "high risk" to the rights and freedoms of individuals following a data breach, the Nursery is also required to notify the individuals affected by the breach. However, in the interests of transparency, the Nursery recognises on some occasions it will be appropriate to notify affected individuals, even if we are not legally obliged to do so.

If the Nursery fails to report a notifiable personal data breach, we are at risk of receiving a sanction from the ICO, which may include a fine. Aside from our desire to avoid receiving any sanctions, the purpose of this policy is to ensure that we protect the Personal Data of our stakeholders and minimise any risks to them following a breach.

The Nursery will ensure staff are trained to recognise and report personal data breaches. Refresher training will be provided at least every two years.

We rely on our staff to be alert to the risk of data security breaches and to follow the procedures set out in this policy to ensure that we can react promptly in the event that a breach or suspected breach occurs. Any member of staff who becomes aware of a suspected or actual personal data breach must follow the escalation procedures set out below. Failure to comply with these procedures may be a disciplinary issue.

The Nursery uses School Consulting Ltd, an External DPO service (advisory).

3. **What is a personal data breach?**

The legal definition of a personal data breach is, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:
-Loss or theft of data or equipment
-People gaining inappropriate access to personal data
-A deliberate attack on systems
-Equipment failure
-Human error
-Acts of God (for example, fire or flood)

Breaches can be categorised according to the following three well-known information security principles:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data

Depending on the circumstances, a breach can relate to the confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

A security incident resulting in personal data being made unavailable for temporary period is also a type of breach, as the lack of access to the data could have a significant impact on the rights and freedoms of data subjects, for example, if our IT system goes down. This type of breach should be recorded in the Nursery's Data Breach Log (within the electronic GDPR folder). However, depending on the circumstances of the breach, it may or may not require notification to the ICO and communication to affected individuals.

Where personal data is unavailable due to planned system maintenance being carried out, this should not be regarded as a 'breach of security'.

4. Understanding the risk to the rights and freedoms of individuals

A breach can potentially have a number of consequences for individuals, which can result in physical, material, or non-material damage. This can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

When assessing the risk to individuals, the Deputy DPO will consider the following factors:
-the type of breach
-the nature, sensitivity, and volume of personal data
-ease of identification of individuals
-severity of consequences for individuals
-special characteristics of the individual
-special characteristics of the data controller, and
-the number of affected individuals.

5. Timescales for reporting a breach

The Nursery is required to report a notifiable breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.

It is likely that the Nursery will be deemed as having become "aware" of a breach when we have a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised. The GDPR expects us to ascertain whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place. This puts an obligation on us to

ensure that we will be “aware” of any breaches in a timely manner so that we can take appropriate action.

While some breaches may be obvious, in other cases we may need to establish whether personal data has been compromised. In such circumstances, we will investigate promptly in accordance with the procedures below to determine whether a breach has happened which, in turn, will enable us to decide if remedial action is needed and if the breach needs to be notified to the ICO and the affected data subjects.

It is possible that we may not have established all of the relevant facts following a data security breach or completed our investigation within 72 hours. However, in the event that the Nursery determines that a breach has taken place and that it needs to be notified to the ICO, a report should be made within 72 hours with the information held at that point in time. In these circumstances, the report to the ICO should explain that further information will be provided as and when it is available.

It is possible that some breaches may come to the attention of a member of staff or may be flagged up by our IT systems. However, it is also possible that we may be notified about breaches by third parties, such as the people who are affected by the breach, a data processor or by the media.

In the event that we investigate a suspected breach and we are able to establish that no actual breach has occurred, the Data Breach Log must still be completed so that we can keep records of ‘near misses’ or other weaknesses in our systems and procedures in order to continuously review and improve our processes.

6. Response plan

Step-by-Step Response Plan (for all staff):
1. Immediately report any suspected or actual breach to the Deputy DPO or via the dpo@ email.
2. Do not attempt to investigate or resolve independently – await instruction.
3. The Deputy DPO will assess and record details in the Breach Log.
4. If in doubt, the External DPO will be consulted, particularly if ICO reporting may be required.
5. Contain the breach where possible (e.g. secure documents, isolate IT systems) following Deputy DPO instructions.
6. Cooperate fully with any investigation or requests for information.
7. Do not contact data subjects directly unless authorised by the Deputy DPO.

A member of staff within the Nursery, who becomes aware of a suspected or actual data security breach, must inform the Deputy DPO (HT) without delay. The email address for contacting the Deputy DPO is dpo@westfieldnurseryNursery.org and the email account is regularly reviewed by the Deputy DPO internally. The External DPO is contacted by the above party as required.

If a member of staff is unsure if a breach has happened, the above procedures must still be followed without delay so that the suspected breach can be investigated in order to establish whether a breach has happened and, if so, whether it needs to be notified to the ICO or the data subjects.

The Deputy DPO will then be responsible for assessing whether the breach or suspected breach needs to be formally escalated to the External DPO. If the Deputy DPO decides not to escalate it to the External DPO, the Data Breach Log must be completed as accurately as possible, including the reasons why the incident does not need to be escalated to the External DPO. The Data Breach Log is reviewed by the External DPO during DPO Inspection Visits. The External DPO must always be informed if there is any doubt whether this would reach the threshold of reporting to the ICO.

If the Deputy DPO decides to escalate a breach or suspected breach to the External DPO, they must do so without delay. Where possible, the Data Breach Log must be completed with as much information as possible. However, if it is not convenient or practicable to complete

the Data Breach Log, the report can be made by setting the information out in an email or over the phone in extreme cases, though a written record is required.

Once a breach or suspected breach has been reported, the Deputy DPO must commence an investigation and assess whether he/she has sufficient information to identify next steps. The purpose of the investigation is to:
-establish if a breach has happened
-establish the nature and cause of the breach
-establish the extent of the damage or harm that results or could result from the breach
-identify the action required to stop the data security breach from continuing or recurring, and
-mitigate any risk of harm that may continue to result from the breach

The Deputy DPO may need to speak to the member of staff who first reported the breach or suspected breach. During the course of his or her investigation, the Deputy DPO should consider whether to involve the Nursery's Data Breach Response Team which consists of: Deputy DPO, SBM, plus other key staff at the Headteacher's request. The External DPO is not part of the response team but may be consulted for technical or regulatory advice where appropriate.

If the Deputy DPO is unavailable for any reason, senior staff must fulfil the responsibilities of the Deputy DPO set out in this Data Breach Response Plan. The Headteacher must have access to the email account identified above to which data breaches are reported.

If the Deputy DPO decides to involve the Data Breach Response Team, the above individuals will be copied into email correspondence and provided with regular updates on the investigation and response to the incident.

The Deputy DPO should consider whether input is required from the Nursery IT or HR in order to further investigate the incident, including the extent of the incident and whether any steps need to be taken to contain any breach. Contact details for IT support are available in the office and the company used for the support is identified in the Supplier Compliance Log.

Depending on the circumstances, the Headteacher should consider whether the Nursery's insurers should be notified in accordance with policy terms, whether legal advice is required and if the incident needs to be reported to the Police and the Local Authority. The Deputy DPO will also consider if specialist IT support is required in order to contain and manage a breach and whether the county Press Office advisors should be engaged if it is likely that we will need to communicate internally and / or externally with our stakeholders regarding the breach or suspected breach.

If the breach or suspected breach has occurred at one of our Data Processors, the Deputy DPO must liaise with the Data Processor to obtain as much information as possible about the extent of the breach or suspected breach and any steps being taken to mitigate any risk to data subjects. It remains the Nursery's responsibility along with guidance from the Deputy DPO, to decide whether to report any such breach to the ICO within 72 hours. Data Processor breaches must always be escalated to the external DPO, as the Nursery retains legal responsibility.

The same requirement applies if the breach or suspected breach is reported to us by a joint Data Controller though in this case we need to establish with the joint Data Controller who is going to report the breach to the ICO and the data subjects, if such notification is required.

Depending on the timescales as to when a member of staff originally became aware of a breach, the Deputy DPO must be mindful of the requirement to notify the ICO without delay and within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. As stated above, it is therefore possible that a data security breach may need to be reported to the ICO before the Nursery has fully investigated or contained the breach. A report to the ICO must contain the following information:

-the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned
-the name and contact details of the Deputy DPO/Deputy DPO or other contact point where more information can be obtained
-the likely consequences of the personal data breach
-the measures taken or proposed to be taken by the Nursery to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The DPO or Deputy DPO is not required to provide precise details in the report to the ICO if this information is not available and an updated report can be made as and when further details come to light. Such further information may be provided in phases without undue further delay. The DPO or Deputy DPO should inform the ICO if the Nursery does not yet have all the required information and if further details will be provided later on.

If a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred, this information could then be added to the information already given to the ICO and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

In the event that a notifiable breach is not reported to the ICO within 72 hours, a report should be made without delay with the reasons for the delay.

If the Deputy DPO concludes that a referral to the ICO is required and also concludes there is likely to be a high risk to the rights and freedoms of individuals resulting from the data security breach, then the data subjects affected by the breach must also be notified without undue delay.

The Deputy DPO must liaise with the Headteacher in relation to how the issue should be communicated to the relevant stakeholders. The Nursery should consider which is the most appropriate way to notify affected data subjects, bearing in mind the security of the medium as well as the urgency of the situation. The notice to the affected individuals should contain the following information: All external communications (letters to parents, media responses) must be cleared by the Headteacher and Deputy DPO before issue, and the external DPO may provide wording or review if requested.
-description of the nature of the breach
-the name and contact details of the Deputy DPO or other contact point
-a description of the likely consequences of the breach, and
-a description of the measures taken or proposed to be taken by the Nursery to address the breach, including, where appropriate, measures to mitigate its possible adverse effects

Given that a large number of our stakeholders are children, if a data breach affects our pupils, the above information may need to be given to parents / carers for affected pupils.

If the Deputy DPO/DPO decides to notify data subjects about a breach, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed by the breach should also be included. The Nursery should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

The Deputy DPO must complete the Data Breach Log before making the referral to the ICO and keep it under review as and when further information comes to light.

In certain circumstances, where justified, and on the advice of law-enforcement authorities, the Nursery may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

Even if the Deputy DPO initially decides not to communicate the breach to the affected data subjects, the ICO can require us to do so, if it considers the breach is likely to result in a high risk to individuals.

In the event that the Deputy DPO concludes it is not necessary to refer the breach to the ICO, the Deputy DPO must still complete the Data Breach Log and clearly set out the reasons why the Deputy DPO or Deputy DPO is satisfied that a referral is not required. The Nursery must keep the decision under review and prepare to make a referral to the ICO if any circumstances change, or if any information comes to light which means that a referral should be made.

Once the breach has been contained and action taken to stop or mitigate the breach, the Deputy DPO or DPO must then review the incident and identify any steps which need to be taken in order to prevent a similar breach occurring in future. This may also include whether any disciplinary action is required against any members of staff or pupils.

As part of the review process, the Nursery should undertake an audit which should include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed. The audit should include an assessment of any ongoing risks associated with the breach and evaluate the Nursery response to it and identify any improvements that can be made. The review should also consider the effectiveness of this Data Breach Response Plan and whether any amendments need to be made to it.

Where security is found not to be appropriate, the Deputy DPO should consider what action needs to be taken to raise data protection and security compliance standards and whether any staff training is required.

Where a data processor caused the breach, the Deputy DPO should consider whether adequate contractual obligations were in place to comply with the GDPR and if so, whether the data processor is in breach of contract.

7. Record Keeping

Record Keeping logs will be kept for a period of 6 years from the date of the incident. This aligns with the Nursery's data retention schedule.

The Data Protection Officer checks processes and controls at least annually and logs of Data Risk, Data Breaches, Subject Access Requests are maintained by the Nursery and subject to inspection and interrogation during DPO visits.

8. Nursery holidays

The Nursery recognises there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because the Nursery is closed and have limited staff available during Nursery holidays. A breach may still occur during these periods, and we will implement the following steps to mitigate any risk caused if a breach happens during the Nursery holidays:

-The DPO@ email address will be made available to staff and will be available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur. This email address will be monitored regularly by the assigned member of staff.

-The Deputy DPO will have the contact details for the Data Breach Response Team so action can be taken without delay, should a breach occur.

-The Deputy DPO should follow the steps set out above as best as they can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the Nursery is closed and has limited staff available due to the Nursery holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the Nursery should take to mitigate any risks.

9. How do we protect our data?

Our data backup and security measures are documented in the Supplier Compliance Evidence folder; part of the GDPR folder within the Nursery central electronic filing system, accessible by senior and key support staff. This organisation, responsible for data backup has detailed the current security measures and storage processes/methods. Any changes to this system or procedure will be evident by an updated version number of that document.

10. Contact for IT Support

Partnership Education
https://partnership.education/
Tel: 01234 436156

11. Monitoring and Review

This Data Breach Response Plan will be kept under review by the Deputy DPO and may be revised to reflect good practice or changes to our organisational structure.

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. This policy will be reviewed every two years by the Headteacher– the next scheduled review date for this policy is May 2028. Any changes made to this policy will be communicated to all members of staff and the governing board.