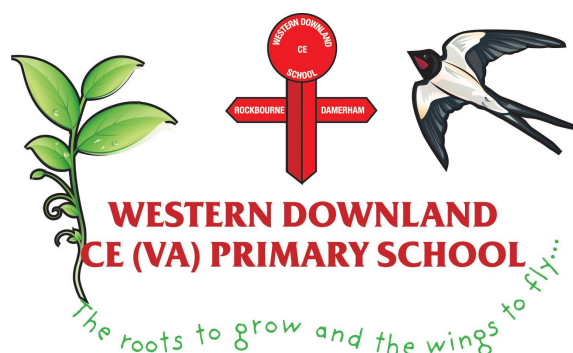


Western Downland CofE (Aided) Primary School Data Protection policy (Including the Protection of Biometric Information)



**Approved by:
Governing Body**

Date: May 2023

**Last reviewed
on:** September 2026

**Next review due
by:** September 2027

Contents

1. **Aims**
2. **Legislation and Guidance**
3. **Definitions**
4. **The Data Controller**
5. **Roles and Responsibilities**
 - 5.1 Governing Board
 - 5.2 Data Protection Officer (DPO)
 - 5.3 Headteacher
 - 5.4 All Staff, Governors and Volunteers
6. **Data Protection Principles**
7. **Collecting Personal Data**
 - 7.1 Lawfulness, Fairness and Transparency
 - 7.2 Special Category Personal Data
 - 7.3 Limitation, Minimisation and Accuracy
8. **Sharing Personal Data**
 - 8.1 Sharing with External Organisations
9. **Subject Access Requests and Other Rights of Individuals**
 - 9.1 Subject Access Requests (SARs)
 - 9.2 Requests Relating to Children's Information
 - 9.3 Refusing or Limiting Requests
10. **Parental Requests to Access Educational Records**
11. **Biometric Recognition Systems**
12. **Photographs and Videos**
13. **Artificial Intelligence (AI) Systems**
14. **Data Protection by Design and Default**
15. **Data Security and Storage of Records**
16. **Disposal of Records**
17. **Personal Data Breaches**
18. **Data Breach Response Procedure**
 - Step 1 – Report the Breach
 - Step 2 – Contain the Breach
 - Step 3 – Assess the Risk
 - Step 4 – Report and Notify
 - Step 5 – Review and Improve
19. **Training**
20. **Monitoring and Review Arrangements**
21. **Links with Other Policies**

Appendix 1: Personal Data Breach Procedure

- Reporting a Breach
- Initial Investigation
- Examples of Possible Breaches and Actions

- Confidential Information Sent to the Wrong Person
- Lost or Stolen Equipment Containing Personal Data
- Safeguarding Information Disclosed Incorrectly

1. Aims

Western Downland CE VA Primary School and Little Foresters Nursery is committed to protecting the privacy and security of personal information relating to pupils, parents/carers, staff, governors, volunteers, visitors and other individuals.

This policy explains how the school collects, stores, uses and protects personal data in accordance with UK data protection legislation.

This policy applies to all personal data processed by the school, whether held electronically or in paper format.

The school is committed to ensuring that personal data is:

- processed lawfully, fairly and transparently
- collected only for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date where necessary
- retained only for as long as necessary
- stored securely and protected from unauthorised access, loss, misuse or disclosure

The school recognises that protecting personal information is essential to maintaining the trust of pupils, families, staff and the wider school community.

2. Legislation and guidance

This policy complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR), where applicable
- Protection of Freedoms Act 2012 in relation to biometric information
- Education (Pupil Information) (England) Regulations 2005
- Information Commissioner's Office (ICO) guidance relating to data protection compliance
- Department for Education (DfE) guidance relating to data protection and information security in schools

This policy should be read alongside the school's privacy notices, records retention arrangements and related safeguarding and information security policies.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual.
Special category personal data	More sensitive personal data requiring additional protection, including information relating to health, ethnicity, religion, trade union membership, biometrics, genetics and sexual orientation.
Processing	Any activity involving personal data, including collecting, recording, storing, using, sharing, altering or deleting information.
Data subject	The individual whose personal data is being processed.
Data controller	The organisation that determines the purposes and means of processing personal data.
Data processor	An organisation or individual that processes personal data on behalf of the data controller.
Personal data breach	A security incident resulting in accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data.
Data Protection Impact Assessment (DPIA)	A process used to identify and reduce privacy risks before introducing new processing activities.

4. The Data Controller

Western Downland CE VA Primary School and Little Foresters Nursery is the data controller for the personal information it processes.

The school determines how and why personal data is processed and is responsible for ensuring that processing complies with UK GDPR and the Data Protection Act 2018.

The school has registered with the Information Commissioner's Office (ICO) where required and complies with its obligations as a data controller.

The school will ensure that:

- personal data is processed fairly and lawfully
- individuals are informed about how their information is used
- appropriate security measures are in place
- staff understand their responsibilities when handling personal information
- data protection risks are considered when introducing new systems or processes

5. Roles and responsibilities

This policy applies to:

- all employees of the school

- governors
- volunteers
- contractors
- visitors
- external organisations processing information on behalf of the school

Anyone who fails to comply with this policy may be subject to disciplinary action or other appropriate measures.

5.1 Governing Board

The Governing Board has overall responsibility for ensuring that the school complies with its legal obligations relating to data protection.

The Governing Board will:

- ensure appropriate data protection policies and procedures are in place
- monitor compliance with UK GDPR requirements
- receive reports relating to significant data protection issues
- ensure appropriate resources are available to maintain compliance
- ensure that data protection responsibilities are understood across the school

5.2 Data Protection Officer (DPO)

The Data Protection Officer oversees the school's compliance with data protection legislation and provides advice and guidance on data protection matters.

The DPO will:

- advise the school on data protection responsibilities
- monitor compliance with UK GDPR requirements
- advise on Data Protection Impact Assessments (DPIAs)
- support staff with data protection queries
- maintain records of personal data breaches
- act as a point of contact for individuals regarding data protection matters
- act as a point of contact for the ICO

The DPO will provide information about significant data protection matters to the Governing Board where appropriate.

Data Protection Officer:

Mrs Alice Tubbs

Email:

a.tubbs@westerndownland.hants.sch.uk

Telephone:
01725 518233

5.3 Headteacher

The Headteacher is responsible for ensuring that this policy is implemented on a day-to-day basis.

The Headteacher will ensure that:

- staff follow data protection procedures
- appropriate security measures are maintained
- concerns and breaches are reported appropriately
- staff receive appropriate training

5.4 All staff, governors and volunteers

Everyone who has access to personal data is responsible for ensuring it is handled securely and appropriately.

Individuals must:

- process personal data in accordance with this policy
- only access information required for their role
- keep personal information secure
- maintain confidentiality
- report mistakes, concerns or suspected breaches immediately
- complete required data protection training
- follow school procedures when using technology and information systems

Staff must contact the DPO if they:

- are unsure whether they have a lawful basis for processing information
- need advice about sharing information
- receive a subject access request
- are unsure about consent requirements
- identify a suspected data breach
- are introducing a new system or process involving personal data

6. Data protection principles

UK GDPR sets out seven key principles that organisations must follow when processing personal data.

The school will ensure that personal data is processed in accordance with these principles.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner.

The school will ensure that individuals understand:

- what information is collected
- why it is collected
- how it will be used
- who it may be shared with

Purpose limitation

Personal data will only be collected and used for specified, explicit and legitimate purposes.

Information collected for one purpose will not be used for an unrelated purpose unless there is a lawful basis to do so.

Data minimisation

The school will only collect and process personal data that is adequate, relevant and necessary for the purpose for which it is required.

Staff must not collect or retain information that is unnecessary.

Accuracy

The school will take reasonable steps to ensure that personal data is accurate and kept up to date.

Individuals are encouraged to inform the school of any changes to their personal information.

Storage limitation

Personal data will not be kept for longer than is necessary.

Retention periods are determined by:

- statutory requirements
- legal obligations
- operational needs
- recognised education retention guidance

The school follows its Records Retention Schedule.

Integrity and confidentiality (security)

Personal data must be protected against:

- unauthorised access

- accidental loss
- unlawful disclosure
- misuse
- alteration or destruction

The school will use appropriate technical and organisational measures to protect information.

Accountability

The school is responsible for demonstrating compliance with UK GDPR requirements.

The school will maintain appropriate records, procedures and evidence of compliance.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The school will only process personal data where there is a lawful basis under UK GDPR.

The lawful bases used by the school may include:

Contract

Where processing is necessary to fulfil employment or service agreements.

Legal obligation

Where the school is required to process information by law.

Vital interests

Where processing is necessary to protect someone's life.

Public task

Where processing is necessary for the school to carry out its public functions and responsibilities.

Legitimate interests

Where processing is necessary for legitimate purposes and individual rights are not overridden.

Consent

Where an individual has freely provided permission for specific processing activities.

Where consent is relied upon:

- it must be freely given, informed and specific
- individuals must understand what they are consenting to
- individuals must be able to withdraw consent at any time

7.2 Special category personal data

Special category personal data requires additional protection.

Where the school processes special category data, it will identify both:

- a lawful basis under Article 6 of UK GDPR; and
- an additional condition under Article 9 of UK GDPR

This may include:

- employment, social protection or social security obligations
- substantial public interest
- health or occupational purposes
- explicit consent where appropriate

Examples of special category information processed by schools may include:

- medical information
- disability information
- safeguarding information
- ethnicity
- religious beliefs where relevant

7.3 Limitation, minimisation and accuracy

The school will:

- only collect information needed for legitimate purposes
- explain why information is collected
- ensure information is accurate and updated where necessary
- securely delete information when it is no longer required

Staff must only access and use personal data necessary for their role.

Personal information must be retained and disposed of in accordance with the school's Records Retention Schedule.

8. Sharing personal data

The school will only share personal data where there is a lawful basis to do so.

Consent will not normally be required where information sharing is necessary to fulfil a legal duty or protect individuals.

Personal data may be shared where:

- there is a legal requirement
- sharing is necessary to safeguard a child or adult at risk
- another organisation provides services on behalf of the school
- emergency services require information

- government departments require information for statutory purposes
- sharing supports the education or wellbeing of pupils

8.1 Sharing with external organisations

When sharing personal data with external organisations, the school will ensure:

- appropriate checks are completed
- information is shared securely
- only necessary information is disclosed
- contracts or agreements are in place where required
- processors comply with UK GDPR requirements

The school may share information with organisations including:

- Hampshire County Council
- Department for Education (DfE)
- Ofsted
- health services
- social care organisations
- safeguarding partners
- examination and awarding bodies
- approved IT providers
- professional advisers
- emergency services
- law enforcement agencies

Information will only be shared on a need-to-know basis and appropriate safeguards will be applied.

9. Subject access requests and other rights of individuals

Individuals have rights under UK GDPR regarding the personal information held about them.

Individuals may have the right to:

- confirm whether their personal data is being processed
- access a copy of their personal data
- understand how their information is used
- know who their information has been shared with
- understand how long information will be retained
- request correction of inaccurate information

- request restriction of processing in certain circumstances
- object to certain types of processing
- request deletion of information where applicable
- receive information about automated decision-making
- complain to the Information Commissioner's Office (ICO)

All requests must be forwarded immediately to the Data Protection Officer.

9.1 Subject Access Requests (SARs)

A Subject Access Request is a request from an individual for access to the personal data the school holds about them.

A request may be made:

- verbally; or
- in writing

To help the school respond efficiently, individuals are encouraged to provide:

- their name
- contact details
- details of the information requested
- relevant dates or information to help locate records

The school may request proof of identity before providing information.

The school will respond without undue delay and normally within **one calendar month** of receiving a valid request.

Where a request is complex or numerous, the school may extend the response period by up to two additional months. The individual will be informed within one month if an extension is required.

9.2 Requests relating to children's information

Personal data relating to a child is the child's personal data.

Parents and carers do not automatically have an absolute right to access all information held about their child.

When considering a request for a child's personal information, the school will consider:

- the child's age and maturity
- whether the child understands their rights
- the child's wishes and views where appropriate
- whether disclosure is in the child's best interests
- whether another person's personal data would also be disclosed

Each request will be considered on a case-by-case basis.

9.3 Refusing or limiting requests

The school may refuse or restrict a request where permitted by law.

This may include where:

- disclosure would cause serious harm to an individual
- information relates to another person and cannot reasonably be disclosed
- legal privilege applies
- the request is manifestly unfounded or excessive

Where a request is refused, the school will explain the reasons and inform the individual of their right to complain to the ICO.

10. Parental requests to access educational records

Parents and those with parental responsibility have a legal right to access their child's educational record under the **Education (Pupil Information) (England) Regulations 2005**.

Requests should be made in writing to the school.

Where a request relates specifically to an educational record, the school will respond within the statutory timeframe.

The school may refuse access where:

- disclosure would cause serious harm to the physical or mental health of the pupil or another person
- the information contains another person's personal data which cannot reasonably be disclosed
- another legal exemption applies

Where a parent requests a copy of an educational record, the school may charge a reasonable fee where permitted by legislation.

Access to educational records is separate from a Subject Access Request made under UK GDPR.

11. Biometric recognition systems

Western Downland CE VA Primary School and Little Foresters Nursery does not currently use automated biometric recognition systems.

If the school introduces a biometric system in the future, it will:

- complete a Data Protection Impact Assessment (DPIA) before implementation
- provide clear information to parents/carers, pupils and staff about how biometric information will be used
- comply with the Protection of Freedoms Act 2012

- ensure biometric information is processed lawfully under UK GDPR
- obtain appropriate consent before collecting biometric information

For pupils:

- written consent from parents/carers will be obtained before biometric information is collected or processed
- pupils will be informed about the system and their choices
- an alternative method will be provided for pupils who do not wish to use the biometric system

Biometric information used for identification or authentication purposes is classed as special category personal data and will receive appropriate protection.

12. Photographs and videos

The school may take photographs and videos of pupils, staff and visitors as part of school activities.

Photographs and videos may be used for:

- celebrating achievements
- recording educational activities
- school displays
- newsletters and publications
- communication with parents and the wider community
- the school website
- approved social media platforms
- promotional materials

Where photographs or videos identify individual pupils, the school will ensure that an appropriate lawful basis is identified.

Where consent is used as the lawful basis:

- consent will be obtained from parents/carers where required
- parents/carers may refuse consent
- consent may be withdrawn at any time

Where consent is withdrawn, the school will take reasonable steps to stop future use of the images and remove them from future publications where possible.

Staff must not use personal devices to take photographs or videos of pupils unless authorised by the school.

Images must only be stored, accessed and shared using approved school systems and procedures.

Parents/carers taking photographs or videos at school events for personal use are not normally covered by UK GDPR. However, the school asks parents/carers to respect the

privacy of other children and not share images containing other pupils publicly without permission.

When publishing photographs or videos, the school will avoid publishing unnecessary personal information alongside images.

13. Artificial Intelligence (AI) systems

The school may use artificial intelligence (AI) systems to support educational, administrative and operational activities.

Where AI systems process personal data, the school will ensure that:

- processing is lawful, fair and transparent
- appropriate safeguards are in place
- personal data shared with AI systems is limited to what is necessary
- confidential and sensitive information is protected
- staff understand how AI tools should and should not be used

Staff must not enter confidential, personal, safeguarding or special category information into publicly available AI systems unless the system has been approved by the school and appropriate safeguards are confirmed.

Staff using AI systems must:

- follow the school's AI guidance
- avoid unnecessary disclosure of personal information
- check AI-generated information for accuracy
- consider bias and reliability
- apply professional judgement
- remain responsible for decisions made using AI-generated information

Where AI systems process personal data, the school will ensure appropriate contracts, security measures and data protection checks are in place.

14. Data protection by design and default

The school will consider data protection from the earliest stage when introducing new systems, technologies, activities or processes.

The school will:

- only collect personal data that is necessary
- ensure privacy considerations are built into new projects and systems
- complete Data Protection Impact Assessments (DPIAs) where processing may create a high risk to individuals
- maintain appropriate records of processing activities

- provide privacy notices to individuals where required
- restrict access to personal information
- provide appropriate training to staff and governors
- regularly review data protection procedures and security arrangements

The Data Protection Officer will advise on proposed activities that may affect individuals' privacy rights.

15. Data security and storage of records

The school takes appropriate technical and organisational measures to protect personal data from:

- unauthorised access
- accidental loss
- accidental or unlawful destruction
- alteration
- inappropriate disclosure
- misuse

All staff, governors, volunteers and contractors who have access to personal data are responsible for keeping it secure.

The school will ensure that:

- paper records containing personal data are stored securely when not in use
- confidential documents are not left unattended in classrooms, offices or shared areas
- access to electronic systems is restricted to authorised individuals
- staff use secure passwords and do not share passwords
- portable devices containing personal data are protected and encrypted where appropriate
- personal data is stored only on approved school systems
- personal information is not sent using personal email accounts unless specifically authorised
- information is not transferred using unapproved methods
- access permissions are reviewed regularly

Where staff or governors access school information remotely, they must follow the same security requirements as when working on school premises.

Any loss, theft, accidental disclosure or suspected compromise of personal data must be reported immediately to the Data Protection Officer.

16. Disposal of records

Personal data that is no longer required will be securely destroyed in accordance with the school's Records Retention Schedule.

When disposing of records, the school will ensure that:

- paper documents containing personal data are securely shredded
- electronic records are securely deleted
- storage devices are securely wiped or destroyed where necessary
- third-party disposal companies provide appropriate assurances that confidential information will be securely destroyed

The school will retain information only for as long as necessary for legal, educational, safeguarding and operational purposes.

17. Personal data breaches

The school aims to prevent personal data breaches. However, where a breach occurs or is suspected, the school will respond promptly and appropriately.

A personal data breach may include:

- personal information being sent to the wrong person
- loss or theft of paperwork or equipment containing personal data
- unauthorised access to personal information
- accidental disclosure of confidential information
- information being altered or deleted without authorisation

Any member of staff, governor, volunteer or contractor who becomes aware of a possible data breach must report it immediately to:

Data Protection Officer

Mrs Alice Tubbs

Email:

a.tubbs@westerndownland.hants.sch.uk

Telephone:

01725 518233

The school will:

- investigate the incident
- assess the level of risk to individuals
- take steps to contain and reduce the impact of the breach
- decide whether the breach must be reported to the Information Commissioner's Office (ICO)
- notify affected individuals where required
- keep a record of all breaches and actions taken

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, the school will notify the ICO within **72 hours of becoming aware of the breach**.

18. Data breach response procedure

If a data breach occurs, the following procedure will be followed.

Step 1 – Report the breach

The person who discovers or suspects a breach must immediately inform the Data Protection Officer.

Examples include:

- sending personal information to the wrong recipient
- losing a laptop, tablet or paper file containing personal information
- sharing confidential information without permission
- allowing unauthorised access to school systems

The breach must be reported even if the person is unsure whether it meets the definition of a personal data breach.

Step 2 – Contain the breach

The Data Protection Officer will work with relevant staff to:

- recover information where possible
- stop further unauthorised access
- secure affected systems
- contact third parties where necessary
- take immediate steps to reduce potential harm

Step 3 – Assess the risk

The Data Protection Officer will consider:

- what information has been affected
- whose information has been affected
- how many individuals are involved
- the sensitivity of the information
- the potential impact on individuals
- whether the breach is likely to result in a risk to individuals' rights and freedoms

Step 4 – Report and notify

Where required:

- the ICO will be notified within 72 hours
- affected individuals will be informed
- safeguarding concerns will be referred to the Designated Safeguarding Lead
- other relevant organisations will be contacted where appropriate

Step 5 – Review and improve

Following a breach, the school will review:

- how the breach happened
- whether procedures need improvement
- whether additional training is required
- whether further security measures are needed

19. Training

All staff, governors and volunteers who handle personal data will receive appropriate data protection training.

Training will cover:

- UK GDPR requirements
- confidentiality responsibilities
- secure handling of personal information
- recognising and reporting data breaches
- acceptable use of technology and digital systems
- safe use of AI tools where relevant

Training will be provided:

- as part of induction for new staff and governors
- when legislation or guidance changes
- when school procedures are updated
- where monitoring identifies a need for additional support

Records of training completion will be maintained.

20. Monitoring and review arrangements

The Data Protection Officer is responsible for monitoring compliance with this policy.

The school will:

- review this policy annually

- review procedures following changes in legislation or guidance
- monitor completion of data protection training
- review data breaches and identify improvements
- review privacy notices and information processing activities
- report significant data protection matters to the Governing Board

This policy will be reviewed and approved by the Governing Board.

Policy reviewed: July 2026

Next review date: July 2027

21. Links with other policies

This Data Protection Policy should be read alongside:

- Freedom of Information Publication Scheme
- Acceptable Use of ICT Policy
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Records Retention Schedule
- Records Management Policy
- CCTV Policy (where applicable)
- Staff Privacy Notice
- Pupil Privacy Notice
- Governor Privacy Notice
- AI Use Guidance (where applicable)
- Complaints Policy

Appendix 1: Personal Data Breach Procedure

Reporting a breach

Any staff member, governor, volunteer or contractor who identifies a suspected breach must immediately notify:

Mrs Alice Tubbs – Data Protection Officer

Email:

a.tubbs@westerndownland.hants.sch.uk

Telephone:

01725 518233

The breach must be reported even where the individual is uncertain whether it meets the definition of a personal data breach.

Initial investigation

The Data Protection Officer will establish:

- what information has been affected
- how the breach occurred
- who has been affected
- whether information has been accessed by unauthorised individuals
- whether immediate action is required

The DPO will record:

- the nature of the breach
- the information involved
- the individuals affected
- actions taken
- decisions made regarding notification

Examples of possible breaches and actions

Confidential information sent to the wrong person

The school will:

- attempt to recall emails where possible
- contact the unintended recipient
- request deletion or return of information
- record the incident
- assess whether notification is required

Lost or stolen equipment containing personal data

The school will:

- report the incident immediately
- establish what information was stored on the device
- consider whether remote access can be disabled
- assess the risk to individuals
- report to the ICO where required

Safeguarding information disclosed incorrectly

The school will:

- inform the Designated Safeguarding Lead
- assess the impact on the child or family
- consider whether safeguarding partners need to be informed
- take steps to prevent recurrence