Riversdale Primary School

A nurturing, ambitious and values led school.

DATA PROTECTION AND INFORMATION SECURITY POLICY

DATE: 10th March 2026

REVIEW DATE: 9th March 2027

INTRODUCTION

Riversdale Primary School is committed to protecting the personal data and confidential information of pupils, staff, parents, governors and members of the wider school community.

The school recognises the importance of handling information lawfully, securely and transparently. Personal data is processed in order to support teaching and learning, safeguard pupils, manage the workforce and fulfil statutory responsibilities.

This policy outlines how the school ensures that personal data is processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and how information is protected through appropriate information security measures.

The school is committed to developing a culture in which all staff understand the importance of protecting personal information and handling data responsibly.

AIMS OF THE POLICY

This policy aims to ensure that:

- personal data is processed lawfully, fairly and transparently
- information is handled securely and responsibly
- staff understand their responsibilities when handling personal data
- personal data is retained only for as long as necessary
- data is disposed of securely when no longer required
- appropriate measures are in place to protect information from loss, misuse or unauthorised access.

LEGAL FRAMEWORK

This policy is based on the requirements of:

- UK General Data Protection Regulation
- Data Protection Act 2018

The school also follows recognised records management guidance applicable to schools.

DATA PROTECTION PRINCIPLES

The school processes personal data in accordance with the following principles:

- Personal data must be processed lawfully, fairly and transparently.
- Data must be collected for specified, explicit and legitimate purposes.
- Data must be adequate, relevant and limited to what is necessary.
- Personal data must be accurate and kept up to date.
- Data must be retained only for as long as necessary.
- Personal data must be processed securely.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Riversdale is committed to ensuring that the data protection principles are embedded into all personal data processing activities. This means that privacy and data protection considerations are integrated into the design of systems, processes and policies from the outset, rather than being addressed retrospectively.

The school will implement appropriate technical and organisational measures to demonstrate that personal data is processed in accordance with data protection legislation.

To achieve this, the school will:

- appoint a suitably qualified Data Protection Officer (DPO) and ensure that they have sufficient independence, resources and access to information to fulfil their duties and maintain up-to-date professional knowledge.
- ensure that personal data is processed only where necessary for specific and legitimate purposes, and that processing is carried out in accordance with the data protection principles set out in relevant legislation.
- undertake Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to the rights and freedoms of individuals, particularly when introducing new systems, technologies or significant changes to data processing activities.
- embed data protection requirements into internal documentation, including this policy, related policies, procedures and privacy notices.

- provide regular training and guidance to staff on data protection responsibilities and maintain appropriate records of training and attendance.
- conduct periodic reviews and audits of data protection practices to ensure that procedures remain effective and compliant.
- maintain records of processing activities in order to demonstrate accountability and transparency.

These records will include:

- the name and contact details of the school and the Data Protection Officer
- details of the types of personal data held by the school
- the categories of individuals whose data is processed
- the purposes for which personal data is used
- details of any third parties with whom data may be shared
- information about how data is stored and secured
- retention periods for different categories of data.

The school will ensure that appropriate privacy notices are made available to individuals explaining how their personal data is collected, used, stored and shared.

Before adopting new digital systems, applications or educational technology platforms that process personal data, the school will undertake appropriate privacy and data protection checks and, where necessary, seek advice from the Data Protection Officer.

ROLES AND RESPONSIBILITIES

Governing Body

The Governing Body acts as the Data Controller and has overall responsibility for ensuring that the school complies with data protection legislation.

Headteacher

The Headteacher is responsible for the day-to-day implementation of this policy and for ensuring that appropriate data protection and information security procedures are in place.

The Headteacher will:

- ensure staff understand their data protection responsibilities
- oversee information security practices across the school
- respond to data protection concerns or incidents
- liaise with the Data Protection Officer where necessary.

Data Protection Officer (DPO)

The school works with the Wandsworth Local Authority Data Protection Officer (DPO) Gary Hipple, who provides advice and guidance on data protection compliance.

The DPO supports the school by:

- advising on data protection matters
- assisting with responses to data breaches
- advising on subject access requests where necessary.

STAFF RESPONSIBILITIES

All staff have a responsibility to ensure that personal data is:

- handled securely
- accessed only where necessary for their role
- shared appropriately and lawfully
- recorded accurately.

Staff must report any concerns relating to data protection or information security to the Headteacher immediately.

INFORMATION SECURITY

The school takes appropriate technical and organisational measures to protect information against unauthorised access, loss, destruction or misuse.

These measures include:

- secure passwords and user authentication
- restricting access to sensitive information
- secure storage of paper records
- use of approved school systems such as Arbor and CPOMS
- ensuring that devices containing school information are password protected.

Staff must not store personal data on unauthorised devices or share school information using personal email accounts.

USE OF PERSONAL DEVICES AND REMOTE WORKING

Staff may occasionally need to access school information outside the school site in order to carry out professional duties.

Where possible, staff should use school-issued devices when accessing school systems.

If a personal device is used in exceptional circumstances, staff must ensure that:

- the device is password protected
- unauthorised users cannot access the device
- personal data is not stored permanently on the device.

When working remotely, staff must ensure that confidential information cannot be viewed by unauthorised individuals.

SAFEGUARDING INFORMATION SECURITY

Safeguarding information is particularly sensitive and requires the highest level of protection.

Safeguarding records are maintained using secure systems such as CPOMS, and access is restricted to authorised staff.

Staff must ensure that safeguarding information is:

- accessed only for legitimate safeguarding purposes
- handled with strict confidentiality
- not shared inappropriately with unauthorised individuals
- not stored on personal devices.

Safeguarding information must only be shared where necessary to protect the welfare of a child.

USE OF ARTIFICIAL INTELLIGENCE AND DIGITAL TOOLS

Digital tools, including artificial intelligence (AI), may be used to support professional tasks.

Staff must ensure that personal data or confidential school information is not entered into AI tools or digital platforms that have not been approved by the school.

This includes information relating to:

- pupils
- staff
- parents or carers
- safeguarding records
- confidential school information.

Where digital tools are used, staff must ensure that no identifiable personal data is entered into these systems.

USE OF DIGITAL SYSTEMS

The school uses secure digital systems to manage information.

These may include:

- school management systems such as Arbor
- safeguarding recording systems such as CPOMS
- secure communication systems.

Access to these systems is restricted to authorised staff.

DATA SHARING

The school may share personal data where it is necessary and lawful to do so.

This may include sharing information with:
- the Department for Education
- the Local Authority
- safeguarding partners
- external professionals supporting pupils.

Only the minimum necessary information will be shared.

SUBJECT ACCESS REQUESTS

Individuals have the right to request access to personal data held about them.

Requests should be made in writing, stating:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

The school will normally respond within one month in accordance with data protection legislation.

DATA BREACHES

A data breach occurs when personal data is lost, accessed without authorisation, disclosed incorrectly or destroyed accidentally.

Examples include:
- sending information to the wrong recipient
- losing a device containing personal data
- unauthorised access to school systems.

Where a breach occurs:
- The incident must be reported immediately to the Headteacher.
- The school will assess the seriousness of the breach.
- The Data Protection Officer will be consulted where necessary.

Serious breaches may be reported to the Information Commissioner's Office.
Further detail can be found in Appendix 1.

DATA RETENTION

The school retains personal data only for as long as necessary.

Retention periods are set out in the Records Retention Schedule (Appendix 2).

Once records reach the end of their retention period, they must be disposed of securely.

DATA DISPOSAL

The school recognises the importance of securely disposing of personal data once it is no longer required.

Disposal of Paper Records

Paper documents containing personal information must be disposed of securely through:

- cross-cut shredding
- confidential waste bins
- approved confidential waste disposal services.

Documents containing personal data must never be placed in general waste or recycling bins.

Disposal of Electronic Records

Electronic files must be permanently deleted when no longer required.

Staff must ensure that files are deleted from:

- shared drives
- local devices
- cloud storage systems.

Disposal of Emails

Emails containing personal information should be deleted once no longer required.

Staff should regularly review and delete unnecessary emails containing personal data.

Disposal of IT Equipment

Before disposing of electronic devices such as laptops or hard drives, the school will ensure that all data is securely removed.

This may include:

- secure data wiping
- removal of storage media
- specialist data destruction services.

Third-Party Disposal Services

Where confidential waste is disposed of through external providers, the school will ensure the provider is reputable and that secure destruction certification is provided where appropriate.

Staff Responsibilities

All staff are responsible for ensuring that personal data is disposed of securely and in accordance with this policy.

Where staff are unsure about disposal procedures, they should seek guidance from the Headteacher.

CLEAR DESK AND CLEAR SCREEN EXPECTATIONS

Staff are expected to follow clear desk and clear screen practices to protect confidential information.

This includes:

- ensuring confidential documents are not left unattended
- locking computer screens when leaving workstations
- ensuring personal data is not visible to unauthorised individuals.

TRAINING AND AWARENESS

Staff will receive guidance on data protection responsibilities as part of induction and ongoing professional development.

MONITORING AND REVIEW

The school will review data protection and information security practices regularly.

The Governing Body will review this policy annually.

LINKED POLICIES

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Acceptable Use Policy
- Photographic and Video Image Policy
- Parent & Pupil Privacy Notice
- Records Retention Schedule (Appendix 2)

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's admin server.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
      Records of all breaches will be stored on the school's admin server.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Sensitive information being disclosed via the school website/Weduc/Social Media

- Member of staff who discovers the sensitive information to inform the DPO as soon as possible.
- DPO to arrange for information to be removed from the school website or application immediately.
- Parents are informed that sensitive information was available on the website and that action has been taken to remove it.
- DPO to follow data breach protocols.

APPENDIX 2: RECORDS RETENTION SCHEDULE

The school retains records only for as long as necessary to meet legal and operational requirements.

Pupil Records

RECORD TYPE	RETENTION PERIOD	DISPOSAL
Pupil educational record	DOB + 25 years	Secure destruction
Safeguarding records	DOB + 25 years	Secure destruction
SEN records	DOB + 25 years	Secure destruction
Attendance registers	3 years	Secure destruction
Accident records (pupil)	DOB + 25 years	Secure destruction

Staff Records

RECORD TYPE	RETENTION PERIOD	DISPOSAL
Personnel file	6 years after employment ends	Secure destruction
Recruitment records (unsuccessful candidates)	6 months	Secure destruction
DBS records	6 months	Secure destruction
Staff disciplinary records	6 years after employment	Secure destruction

Governance Records

RECORD TYPE	RETENTION PERIOD	DISPOSAL
Governing body minutes	Permanent	Archive
Committee minutes	Permanent	Archive
Complaints records	6 years	Secure destruction

Financial Records

RECORD TYPE	RETENTION PERIOD	DISPOSAL
Financial accounts	6 years	Secure destruction
Payroll records	6 years	Secure destruction
Contracts	6 years after expiry	Secure destruction

Health and Safety Records

RECORD TYPE	RETENTION PERIOD	DISPOSAL
Accident records (staff)	3 years	Secure destruction
Risk assessments	3 years after review	Secure destruction

Curriculum and Operational Records

RECORD TYPE	RETENTION PERIOD	DISPOSAL
Curriculum planning	Until superseded	Secure destruction
School policies	Superseded versions retained 3 years	Secure destruction

Secure Disposal

When records reach the end of their retention period, they will be securely destroyed through:

- confidential shredding
- secure digital deletion
- approved confidential waste services.