KING'S STANLEY C OF E PRIMARY SCHOOL

WHERE WE CARE ABOUT LEARNING AND EACH OTHER

King's Stanley C of E Primary School
Data Protection Policy

Data Controller: King's Stanley C of E Primary School
Headteacher / School Data Protection Lead: Mr Derk van den Broek
Data Protection Officer: Gloucestershire County Council – Schools Data Protection Team
Approved by: Governing Body
Date approved: 1 November 2026
Review date: November 2027, or earlier where legislation or guidance changes
Policy owner: Headteacher

1. Purpose

King's Stanley C of E Primary School is committed to protecting the personal information of pupils, parents, staff, governors, volunteers, visitors and others whose information we process.

Good data protection is an important part of safeguarding, effective governance and maintaining the trust of our school community.

This policy explains how the school collects, uses, stores, shares and protects personal information and how we meet our responsibilities under data protection law.

It applies to all staff, governors, volunteers, contractors and others who process personal information on behalf of the school.

2. Legal framework

The school will comply with current data protection legislation and relevant statutory requirements, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003, where applicable;
- Freedom of Information Act 2000;
- Education (Pupil Information) (England) Regulations 2005;
- relevant education, safeguarding and employment legislation.

The school will have regard to current guidance from the Department for Education (DfE) and Information Commissioner's Office (ICO).

Where legislation or statutory guidance changes, the school will apply the current requirements even where this policy has not yet been formally updated.

3. Data protection principles

The school will ensure that personal information is:

- processed lawfully, fairly and transparently;
- collected for specified and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where necessary;
- kept for no longer than necessary;
- processed securely;
- managed in a way that enables the school to demonstrate compliance.

Personal information will only be accessed by those who have a legitimate reason to use it.

4. Roles and responsibilities

Governing Body

The Governing Body has overall responsibility for ensuring that the school meets its responsibilities as a data controller.

Governors will ensure that appropriate policies, procedures and resources are in place and will receive appropriate assurance regarding data protection compliance.

Headteacher / School Data Protection Lead

The Headteacher, **Mr Derk van den Broek**, is the school's Data Protection Lead and is responsible for the day-to-day implementation of this policy.

The Headteacher will ensure that:

- staff understand their responsibilities;
- appropriate training is provided;
- data protection incidents are reported and managed appropriately;
- data protection is considered when new systems and services are introduced;
- appropriate records and procedures are maintained;
- advice is sought from the DPO where appropriate.

Data Protection Officer

The school purchases the Data Protection Officer service provided by **Gloucestershire County Council's Schools Data Protection Team**.

The DPO provides independent advice, monitors compliance, advises on Data Protection Impact Assessments and supports the school with data protection incidents, complaints and individual rights requests. GCC confirms that its traded service provides the appointed DPO function for subscribing schools.

Schools Data Protection Team
Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Telephone: 01452 583619
Email: schoolsdpo@gloucestershire.gov.uk

Staff

All staff are responsible for protecting personal information.

Staff must:

- follow this policy and associated procedures;
- access information only where required for their role;
- keep passwords and accounts secure;
- use approved school systems;
- share information securely;
- report suspected data breaches immediately;
- complete required data protection and cyber-security training;
- seek advice when unsure.

Serious or deliberate breaches may be dealt with under the school's disciplinary procedures.

5. Personal information we process

The school processes information about pupils, parents, staff, governors, volunteers, applicants, visitors and others connected with the school.

This may include:

- names, addresses and contact details;
- dates of birth and identification information;
- admissions and pupil records;
- attendance and absence;
- attainment and assessment;
- behaviour information;
- safeguarding information;
- SEND information;
- medical, health and allergy information;
- disability information;
- free school meal and pupil premium information;
- photographs and video;
- information relating to trips, clubs and activities;
- IT usage and filtering and monitoring information;
- employment, payroll, pension and HR records;
- recruitment and safer recruitment information;
- DBS information where legally permitted.

Some of this is **special category data**, including information relating to health, ethnicity, religion and other particularly sensitive information.

Such information will receive additional protection and will only be processed where an appropriate lawful condition applies.

6. Lawful processing

The school will identify an appropriate lawful basis before processing personal information.

The main lawful bases used by the school are:

- **public task** – where processing is necessary to carry out the school's official functions;
- **legal obligation** – where the school is required by law to process information;
- **contract** – where processing is necessary for a contract;
- **vital interests** – where processing is necessary to protect someone's life;
- **consent** – where individuals have a genuine choice about whether their information is used;
- **legitimate interests** – in limited circumstances where this is lawful and appropriate.

For most of the school's statutory educational functions, public task or legal obligation will normally be the appropriate basis.

The Data (Use and Access) Act 2025 also introduced **recognised legitimate interests** for certain activities set out in law, including some safeguarding, emergency and crime-prevention purposes. Public authorities cannot use this basis for their normal statutory functions, so public task will usually remain the appropriate basis for school functions.

Consent will not be relied upon where another lawful basis is more appropriate.

7. Children's information and safeguarding

The school recognises that children require particular protection when their personal information is processed.

Information provided directly to pupils about the use of their data will be clear and appropriate to their age and understanding.

Children's privacy will be considered when the school introduces new technology or changes the way information is processed.

Particular care will be taken with:

- safeguarding information;
- health and SEND information;
- photographs and video;
- online services and educational technology;
- artificial intelligence;
- filtering and monitoring;
- profiling and automated decision-making.

Data protection law does not prevent appropriate information sharing where this is necessary to safeguard a child.

Staff must not allow uncertainty about data protection to delay necessary safeguarding action.

Safeguarding information will be shared only where necessary and proportionate and significant information-sharing decisions will be appropriately recorded.

8. School information systems

The school uses a number of approved electronic systems to support education, administration and safeguarding.

These currently include:

- **SharePoint** for school planning and document storage;

- **Insight** for assessment and MyPlan;
- **SIMS Next Gen** as the school management information system;
- **CPOMS** for safeguarding records;
- **Edulink**;
- **ParentPay**;
- **Seesaw**;
- **Securus** as part of the school's filtering and monitoring arrangements.

Before introducing new systems or significantly changing existing systems, the school will consider their data protection and security implications and will seek advice from the DPO where appropriate.

Data Protection Impact Assessments will be completed where required.

The school does not currently use biometric identification systems.

Pupils are not routinely issued with individual school devices to take home.

9. Privacy notices and records

The school will provide clear privacy notices explaining how personal information is used.

Privacy notices will be available for relevant groups, including pupils and parents and the school workforce.

They will explain, where relevant:

- what information is collected;
- why it is used;
- the lawful basis;
- who it may be shared with;
- how long it will be retained;
- individual rights;
- monitoring and automated decision-making;
- how to make a complaint;
- how to contact the school and DPO.

Privacy notices will be reviewed regularly and following significant changes to processing.

The school will also maintain an appropriate **Record of Processing Activities (RoPA)**.

10. Data retention and disposal

Personal information will not be kept for longer than necessary.

The school will maintain or follow an appropriate records retention schedule, taking account of:

- statutory requirements;
- DfE guidance;
- safeguarding responsibilities;
- operational need;
- legal and regulatory requirements.

Records will be securely deleted or confidentially destroyed when they are no longer required.

Where pupils transfer to another school, required pupil records will be transferred securely in accordance with legal requirements.

11. Information security

The school will use appropriate technical and organisational measures to protect personal information from loss, damage, unauthorised access or disclosure.

These may include:

- controlled access to systems;
- strong passwords;
- multi-factor authentication where appropriate;
- encryption;
- secure backups;
- filtering and monitoring;
- firewalls and security software;
- software updates and security patching;
- physical security;
- secure disposal;
- staff training.

Staff must use approved school systems when handling personal information.

School information must not normally be forwarded to personal email accounts or stored on unauthorised personal devices.

Staff must take particular care when emailing personal or sensitive information and must check recipients before sending information.

12. Personal devices

School-owned equipment and approved school systems should normally be used when processing school information.

Staff must not routinely use personal mobile phones or other personal devices to photograph or record pupils.

In **exceptional circumstances**, where use of a personal device is necessary and appropriate, staff must:

- ensure there is a legitimate school purpose;
- transfer any required photograph or recording promptly to an approved school system;
- permanently delete it from the personal device as soon as it has been transferred;
- ensure that it is also removed from any automatic personal cloud or photo backup where applicable.

Personal devices must not be used to retain school personal information.

13. Photographs and video

Photographs and videos which identify individuals are personal information.

The school will ensure that an appropriate lawful basis exists for their use.

Consent may be sought where this is appropriate, particularly for public or promotional uses.

The school will maintain appropriate records of photo permissions and will take account of safeguarding restrictions before photographs or video are shared through:

- the school website;
- newsletters;
- social media, including the school's Instagram account;
- promotional materials;
- other public communications.

The school will not publish an identifiable image where doing so would conflict with a safeguarding restriction or other legal requirement.

14. CCTV

The school operates one **Tapo CCTV camera overlooking the school car park**.

Its purpose is to support the security of the school site, vehicles and people using the car park.

The camera is not used for routine monitoring of pupils or staff performance.

The school will ensure that:

- there is a clear purpose for the camera;
- its positioning and field of view are necessary and proportionate;
- appropriate CCTV signage is displayed;
- access to live or recorded footage is restricted to authorised staff;
- footage is stored securely;
- footage is retained only for an appropriate period;
- footage is disclosed to third parties only where there is a lawful reason;
- the use of CCTV is reflected in relevant privacy information;
- the operation of the camera is reviewed periodically;
- a DPIA is completed or reviewed where required.

Audio recording will not be used unless there is a specific and lawful reason to do so.

ICO guidance expects organisations using surveillance to document its purpose, security and retention arrangements and to ensure clear signage is displayed.

15. Filtering and monitoring

The school uses **Securus** as part of its filtering and monitoring arrangements to support safeguarding and online safety.

Information generated through monitoring systems may contain personal or sensitive information.

The school will ensure that:

- monitoring has a clear safeguarding or security purpose;
- access to alerts and reports is limited to authorised staff;
- staff dealing with alerts receive appropriate training;
- information is stored securely;
- appropriate retention arrangements are in place;
- relevant privacy notices explain the monitoring;

- appropriate contractual arrangements are in place with suppliers;
- a DPIA is completed before introducing a new monitoring system or making a significant change where required.

DfE guidance specifically expects access to filtering and monitoring information to be restricted to authorised staff and says schools should consider retention, safeguarding procedures and DPIAs when introducing or significantly changing monitoring systems.

16. Artificial intelligence

The school permits staff to use **Microsoft Copilot** for appropriate professional purposes.

Staff remain responsible for the information they enter into AI systems and for checking the accuracy and suitability of any output.

Personal, confidential, safeguarding, SEND, medical or other sensitive information about identifiable pupils, families or staff must not be entered into an AI system unless that specific processing has been approved by the school and appropriate safeguards are in place.

AI-generated information must not be treated as automatically accurate.

Before approving additional AI services, the school will consider:

- the purpose of the system;
- what information it processes;
- the lawful basis;
- information security;
- retention arrangements;
- supplier use of data, including use for model training;
- international transfers;
- age restrictions;
- children's privacy;
- whether a DPIA is required.

Where automated decision-making has a significant effect on an individual, the school will ensure appropriate safeguards are in place, including the ability to challenge the decision and request human review. This reflects the changes introduced by the DUAA.

17. Data Protection Impact Assessments

A Data Protection Impact Assessment will be undertaken where processing is likely to result in a high risk to individuals' rights and freedoms.

This may include significant new uses of:

- AI;
- EdTech;
- filtering or monitoring;
- CCTV;
- biometric information;
- profiling;
- automated decision-making;
- large amounts of sensitive information.

The DPO will be consulted where appropriate.

Data protection will be considered at the beginning of new projects rather than after systems have been introduced.

18. Suppliers and data processors

Where an external organisation processes personal information on behalf of the school, appropriate checks and written contractual arrangements will be put in place.

The school will consider matters including:

- information security;
- confidentiality;
- use of sub-processors;
- retention and deletion;
- international transfers;
- data breach notification;
- assistance with individual rights requests.

The school remains responsible for ensuring that processors are appointed appropriately.

19. Sharing personal information

Information will only be shared where there is an appropriate lawful basis and sharing is necessary and proportionate.

Depending on the circumstances, information may be shared with organisations including:

- Gloucestershire County Council;
- Department for Education;
- other schools and education providers;
- health services;
- social care;
- safeguarding partners;
- police and law-enforcement bodies;
- assessment organisations;
- payroll and pension providers;
- contracted service providers.

Staff should share only the information necessary for the purpose and should use an appropriate secure method.

Regular or significant information-sharing arrangements will be documented where appropriate.

Requests from the police or other authorities will be considered against an appropriate legal basis rather than information being disclosed automatically.

20. International transfers

Where personal information is stored or processed outside the UK, the school will ensure that an appropriate lawful transfer mechanism is in place.

International processing will be considered when reviewing new suppliers and systems.

21. Individual rights

Individuals have rights in relation to their personal information, subject to legal exemptions and the circumstances of the processing.

These include rights relating to:

- access;
- rectification;
- erasure;
- restriction;
- objection;
- data portability;
- automated decision-making.

Requests do not need to use legal terminology or be made on a particular form.

Staff who receive a request relating to personal information must pass it promptly to the Headteacher.

22. Subject Access Requests

Individuals may request access to personal information held about them.

A Subject Access Request may be made verbally or in writing and does not need to mention GDPR or use the term “subject access request”.

The school will normally respond within **one calendar month**.

Following the Data (Use and Access) Act 2025:

- the school is required to carry out **reasonable and proportionate searches** rather than exhaustive searches;
- where clarification is genuinely required about an unclear request, the response period may be paused while clarification is obtained.

Information concerning other individuals may be withheld or redacted where appropriate.

The school will keep appropriate records of SARs, searches and significant decisions.

23. Pupils and parental access to information

Data protection rights belong to the individual pupil.

A parent does not automatically have a right to make a Subject Access Request for their child simply because they have parental responsibility.

The school will consider the pupil’s age, maturity and understanding when determining whether a pupil can exercise their own rights.

Where appropriate, a parent may act on behalf of a child who does not have sufficient understanding to exercise those rights themselves.

As a maintained school, parents also have a separate statutory right to access their child’s **educational record** under the Education (Pupil Information) (England) Regulations 2005.

A written request to inspect the educational record will normally be dealt with within **15 school days**.

Safeguarding considerations and legal restrictions on disclosure will always be taken into account.

24. Data protection complaints

Anyone who has concerns about how their personal information has been handled may raise a complaint with the school.

Complaints may be made verbally or in writing.

The school will:

- provide a clear and accessible complaints route;
- acknowledge a data protection complaint within **30 days**;
- investigate without undue delay;
- keep the complainant appropriately informed;
- provide an outcome;
- maintain a record of complaints and their resolution.

Complaints should initially be directed to the Headteacher or the school's DPO.

Individuals may also raise concerns with the ICO after the school has had an appropriate opportunity to consider the matter.

The 30-day acknowledgement requirement is one of the specific changes schools are required to incorporate following the DUAA.

25. Personal data breaches

All actual or suspected personal data breaches must be reported **immediately** to the Headteacher.

Examples include:

- information sent to the wrong recipient;
- lost or stolen documents or devices;
- unauthorised access to systems;
- information accidentally published;
- cyberattacks;
- inappropriate access by a member of staff;
- accidental loss or deletion of information.

The school will:

1. contain the incident where possible;
2. establish what information is affected;
3. assess the risk to individuals;
4. involve the DPO where appropriate;
5. record the incident and decisions;
6. take corrective action.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the school will notify the ICO without undue delay and, where feasible, within **72 hours of becoming aware of the breach**.

Where the risk to an individual is high, the affected individual will also normally be informed unless an applicable legal exception applies.

All breaches will be recorded, including those which do not require notification to the ICO.

26. Training and compliance

Staff handling personal information will receive appropriate data protection training as part of induction and regular refresher training.

Additional guidance will be provided for staff working with particularly sensitive information or higher-risk systems.

Governors will receive appropriate data protection awareness.

The school will monitor compliance through measures including:

- DPO advice and reviews;
- staff training;
- breach and complaint records;
- SAR records;
- reviews of privacy notices;
- DPIAs;
- retention arrangements;
- supplier contracts;
- access controls.

27. Associated policies and procedures

This policy should be read alongside relevant school documents, including:

- Safeguarding and Child Protection Policy;
- Acceptable Use Policy;
- Online Safety arrangements;
- Filtering and Monitoring procedures;
- Freedom of Information arrangements;
- Records Retention Schedule;
- Staff Code of Conduct;
- Complaints Policy;
- privacy notices;
- data breach procedure;
- Subject Access Request procedure;
- Record of Processing Activities;
- DPIA process;
- relevant cyber-security procedures.

These operational documents provide the detailed processes which support this policy.

28. Review

This policy will be reviewed annually and sooner where required by:

- changes to legislation;
- significant DfE or ICO guidance;
- changes to the way the school processes information;

- a significant data protection incident;
- advice from the DPO.

Approved by: Governing Body
Date approved: November 2026
Next scheduled review: November 2028

Data Protection Officer contact details

Schools Data Protection Team
Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Telephone: 01452 583619
Email: schoolsdpo@gloucestershire.gov.uk

This is the version I would now use as the school's main policy. The only areas I would deal with separately rather than making this longer are the **CCTV retention/storage detail**, your **records retention schedule**, and the exact operational procedure for SARs and breaches. Those are better kept as supporting documents and can be updated without taking the whole policy back through governors.