St Joan of Arc School
Growing together

Policy

Data Protection

2025-26

((UPDATED TO REFLECT THE DATA (USE AND ACCESS) ACT 2025 (DUAA) AMENDMENTS TO UK GDPR, DPA 2018 AND PECR; PHASED COMMENCEMENT 2025–26)

Mission Statement

The Members of the Community of St Joan of Arc School, by respecting each other, learn and grow in the love of Christ.

Data Protection Policy (updated for UK GDPR)

Policy Reference:	St Joan of Arc
Description:	This document ensures compliance with UK GDPR, DPA 2018, and the Data (Use and Access) Act 2025 (DUAA). DUAA is an upgrade, not a new regime — core principles and safeguarding duties remain unchanged.
Status:	Statutory Policy
Policy Audience:	Governing body and staff
School Contact:	Headteacher
Other related School policies and procedures:	Statutory and non-statutory policies
Governor Committee:	NAME OF COMMITTEE
Approved by Governing Body:	*Spring 2026*
Frequency of review:	Every two years
Latest Date for Next Review:	Summer Term 2027
Version	SP.011 version 03
Policy Level	**Policy Level 2** Statutory Policy (ALL Schools should adopt with no change allowed to core text. Changes to school name and school's usual sign-off and review date reminders allowed)

In reviewing this policy, the Governing Body has had regard to the Equality Act 2010 including amendments introduced by the **Equality Act 2010 (Amendment) Regulations 2023** and carried out an equality impact assessment. It is satisfied that no group with a protected characteristic will be unfairly disadvantaged by this policy.

Data Protection Policy (UK GDPR Update)

Contents

Data Protection Policy (UK GDPR Update)

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation & Guidance

This policy meets the requirements of the UK GDPR, the Data Protection Act 2018 (DPA 2018), and the Privacy and Electronic Communications Regulations (PECR), as amended by the Data (Use and Access) Act 2025 (DUAA). Most of the DUAA changes to UK GDPR and PECR commenced on 5 February 2026, with the statutory controller complaints duty commencing on 19 June 2026. We will keep this policy under review as ICO guidance is updated during 2026.
DUAA introduces changes to DSAR handling, the controller complaints process, cookies/PECR, recognised legitimate interests (RLI), automated decision making (ADM), research/statistical processing, and the charity soft opt-in (where applicable, e.g. academy trusts and charities).

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Significant automated decision	A decision based solely on automated processing that produces a legal effect or similarly significant effect on an individual. DUAA requires specific safeguards and restricts the use of special category data for such decisions
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Recognised Legitimate Interests (RLI)	A statutory list of purposes under DUAA/UK GDPR Article 6(1)(ea) and Annex 1 where no balancing test is required, use only where strictly necessary for: public-task disclosure; national/public security & defence; emergencies; crime (prevention/investigation/apprehension/prosecution); and safeguarding vulnerable individuals

4. The Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the Information Commissioner's Office (ICO) and will renew this registration annually or as otherwise legally required.

5. Roles & Responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing body and, where relevant, report to the body their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the Information Commissioner's Office (ICO).

Full details of the DPO's responsibilities are set out in their job description.

Our DPO's contact details are below:

Barbara van Kan
St Joan of Arc Catholic Primary School
Northolme Road
London
N5 2UX
Email: bvankan@st-joanofarc.islington.sch.uk
Telephone: 020 7226 3920

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting Personal Data

a. Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual’s rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**
- In limited cases set out in UK GDPR as amended by the Data (Use and Access) Act 2025, we may rely on a **recognised legitimate interest** where strictly necessary for one of the purposes (e.g., responding to a public authority’s public task request to disclose data; preventing/detecting crime; safeguarding vulnerable individuals; responding to an emergency; or national/public

security/defence). Recognised legitimate interests do not cover general commercial purposes such as intra-group administration or network and information security, which remain subject to the usual Legitimate Interests Assessment where relied upon under Article 6(1)(f).

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018 (DPA 2018).

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Where applicable, we will follow DUAA clarifications on research and statistical processing and broad consent and ensure appropriate safeguards and transparency.

b. Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud

- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- DUAA introduces statutory recognised legitimate interests for certain disclosures (e.g., responding to requests from bodies performing a public task, emergencies, preventing/detecting crime, safeguarding). Where appropriate, we will document reliance on RLI in our records of processing and data sharing agreements, ensuring necessity and purpose limits are met.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

The school may share pupil data with NHS or local authority immunisation teams under the lawful basis of public task and legal obligation. Only the minimum necessary data will be shared, and appropriate safeguards will be in place.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

We will use appropriate transfer tools (e.g., IDTA or the UK Addendum to the EU SCCs) and conduct Transfer Risk Assessments, applying the UK's revised 'data protection test' (that protections are not materially lower than UK standards). We will follow the ICO's updated international transfers guidance.

9. Subject Access Requests and other Rights of Individuals

a. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- 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.

• Reasonable and proportionate search: We will provide the confirmation, copy and information that we can locate from a reasonable and proportionate search. We will log systems/custodians/date ranges queried and the rationale for any

exclusions. When determining what is reasonable and proportionate, we consider the circumstances of the request, the volume of information that may need to be searched, any difficulties in finding the information, and the fundamental nature of the right of access.

- Pausing the time limit ("stop-the-clock"): We may pause the one month response period while (a) verifying identity, or (b) clarifying scope. Time resumes once we receive what is needed.
- We may extend the period by up to two months for complex or multiple requests and may refuse or charge a reasonable fee where a request is manifestly unfounded or excessive.

b. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12:
Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above:
Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

c. Responding to subject access requests

When responding to requests, we:

- We will respond without undue delay and within one month of receipt (subject to any permitted pause noted above)
- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- Will provide confirmation, copies and information to the extent available from a reasonable and proportionate search. We will document the systems and custodians queried, relevant date ranges, and the rationale for any exclusions. Where appropriate, we will explain any limits applied to the search. When deciding proportionality, we consider: the circumstances of the request; the volume potentially in scope; any difficulties in finding the information; and the fundamental nature of the right of access.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is manifestly unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the Information Commissioner's Office (ICO).

d. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the UK
- For significant automated decisions, we will:
  (a) inform the individual that the decision was automated.
  (b) provide a clear route to make representations, challenge the decision and obtain meaningful human review; and
  (c) ensure appropriate testing, oversight and DPIA are in place. We will not base such decisions on special category data unless a UK GDPR condition permits it and safeguards apply.

- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the Information Commissioner's Office (ICO)
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- The school will ensure that third-party data is redacted appropriately before responding to SARs.
- Staff will be trained to recognise and escalate SARs promptly.
- The school will maintain a log of SARs and responses to demonstrate compliance.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see Educational Record

Parents have a right to access their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. The school may charge a fee for hard copies.

11. Biometric Recognition Systems

If and where the school uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). If a biometric system is introduced, we will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in a school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

The School may use CCTV in various locations around the school site to ensure it remains safe. Where the school uses CCTV, we will adhere to the Information Commissioner's Office (ICO)'s code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Data Protection Officer (DPO)

13. Photographs & Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Pupils aged under 18 years of age
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
Pupils aged 18 years and over
We will obtain written consent from parents/carers, or pupils aged 18 and over, for

photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

14. Data Protection by Design & Default

Under DUAA, the UK permits solely automated decisions with legal/similarly significant effects in wider circumstances, provided safeguards are in place, we will:

(i) inform the individual that the decision was automated.
(ii) provide a clear route to make representations, challenge the decision and obtain meaningful human review; and
(iii) ensure appropriate testing, oversight and DPIA are in place. We will not base such decisions on special category data unless a UK GDPR condition permits it and safeguards apply.

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- DPIAs will be conducted for any processing likely to result in a high risk to individuals rights and freedoms, including new technologies, largescale data processing, or profi ling activities (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- For online services likely to be accessed by children, we will explicitly consider how to protect and support children by design and align with the ICO's Children's Code.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods (in accordance with the IRMS toolkit) and how we are keeping the data secure

15. Use of Generative AI Tools

This section applies to the use of generative AI tools such as Microsoft Copilot, ChatGPT, or similar technologies that generate content based on user input. These examples are illustrative and not exhaustive.

In line with guidance from the Department for Education (DfE), schools may use generative AI tools to support teaching and administrative tasks, such as lesson planning, resource creation, marking, and feedback. However, AI must not replace teachers or be used to make decisions that significantly affect pupils without appropriate human oversight. Schools are responsible for ensuring that any use of AI complies with data protection, safeguarding, and intellectual property laws. The use of AI by pupils is at the school's discretion and must align with the school's acceptable use, academic integrity, and safeguarding policies.

Reference: Department for Education, "Generative Artificial Intelligence (AI) in Education", updated June 2025.

Where generative AI tools are used in school operations or teaching, the school will:

1. Conduct a Data Protection Impact Assessment (DPIA) before use. *See Section 14: Data Protection by Design & Default for more on DPIAs.*
2. Avoid inputting identifiable personal data into AI tools, especially public-facing models.
3. Ensure transparency with staff, pupils, and parents about how AI is used, including disclosing AI-generated content where appropriate.
4. Ensure ethical use of AI: AI must not replace human judgment in decisions with legal or significant effects.
5. Require meaningful human involvement in any decision making process involving AI. *(This aligns with the DUAA's automated decision making framework, which permits significant automated decisions where statutory safeguards are applied (transparency, ability to make representations, human intervention and contest the decision). Special category data must not be used for solely automated significant decisions unless strict legal conditions are met).*
6. Ensure "meaningful human involvement" is substantive: reviewers must be trained, able to challenge or override the output, and records of interventions and spot checks must be maintained.
7. Promote fairness: AI systems must be designed and deployed to avoid discriminatory or inequitable impacts.
8. Ensure privacy: AI tools must not collect, store, or access personal data without consent or another lawful basis.

9. Implement robust security measures to protect AI systems and data from unauthorised access or breaches.
10. Update privacy notices to reflect the use of AI tools where personal data is processed.
11. Maintain governance oversight through appropriate review and approval processes for AI use cases.
12. Provide training to staff on the ethical and responsible use of AI, including data protection implications.
13. Document the use of AI in outputs where applicable, e.g., *"This document was generated in part using Microsoft Copilot 365."*
14. Outputs generated by AI tools may contain inaccuracies, outdated information, or biased content. Staff must critically review all AI-generated material before use and remain responsible for its accuracy and appropriateness. The use of generative AI tools must comply with all applicable data protection laws, including the UK GDPR and the Data Protection Act 2018. Staff remain fully accountable for any content created or decisions made using AI tools. The use of AI does not transfer responsibility away from the individual or the school. Where AI tools are being piloted or evaluated, their use is subject to ongoing review and must follow any guidance issued by the school or governing body.

16. Data Security & Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- We follow NCSC guidance:
  - Use three random words passphrases for strong, memorable passwords.
  - Avoid routine forced password changes (unless compromise is suspected).
  - Enforce multi-factor authentication (MFA) for all cloud services and remote access, preferring phishing-resistant MFA where feasible.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety policy on acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17. Disposal of Records

The school maintains a data retention schedule in line with the Information and Records Management Society (IRMS) toolkit 2024. This schedule outlines how long different types of personal data are retained and ensures data is not kept longer than necessary.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. For more detailed operational guidance, staff should refer to the school's full Data Breach Procedure document.

When appropriate, we will report the data breach to the Information Commissioner's Office (ICO) within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

19. Data protection complaints process

The statutory duty to offer a direct data protection complaints route applies from 19 June 2026; we are operating this process now as good practice.

- We provide accessible routes for individuals to raise data protection complaints to the school (including an electronic form, email and alternative channels). We will:

  • acknowledge each complaint within 30 days of receipt.
  • take appropriate steps without undue delay, including making enquiries and keeping the complainant informed of progress; and
  • communicate the outcome without undue delay.

- Individuals should use the school's complaints route before escalating to the ICO. The school will maintain a complaints register to evidence handling and outcomes.

20. Cookies and similar technologies (PECR)

This section applies to our websites and apps (cookies and similar technologies) and to any electronic direct marketing we send. It does not cover PECR breach-reporting duties for public electronic communications service providers (telecoms/ISPs).

The DUAA's limited cookie exemptions are now in force (commenced 5 Feb 2026). We will apply an exemption only where strictly within scope (e.g. certain low risk analytics used solely to improve the service, or functionality improvements) and otherwise obtain prior consent for non-essential technologies. "Reject all" will be as easy as "Accept all", and non essential tags will not fire until consent is recorded. We will maintain an inventory and remove any technology that exceeds the stated purpose.

Our websites and online services follow PECR as amended by DUAA. We will:

• separate low risk analytics used solely to improve the service or website from any advertising/attribution tags (which remain consent based).

• provide clear information and a visible one step opt-out where relying on an exception.

• assess “instigation” risk (we are responsible for tags/scripts we deploy, even if set by third parties); and

• keep cookie and tag inventories under review and remove any technology that exceeds the stated exception purpose.

We note that PECR fines now align with UK GDPR levels. We will ensure compliance and cooperate with ICO guidance updates.

21.Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school’s processes make it necessary.

22. Privacy Notices

The school will provide clear and accessible privacy notices to individuals at the point of data collection, explaining how their data will be used, stored, and shared. These notices will be reviewed regularly and updated as necessary.

We will update privacy notices when DUAA related changes affect how we process personal data and will follow ICO guidance as it is updated during the DUAA commencement period. We will reflect RLI/ADM in relevant notices.

23. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated as necessary. Otherwise, this policy will be reviewed every 2 years and shared with the full governing body.

24. Links with Other Policies

This data protection policy is linked to other policies including:

- Freedom of information policy (Including publication scheme)
- This policy section applies to the school’s websites and apps (cookies and similar technologies) and to any electronic direct marketing we send (emails, SMS, push notifications, social media direct messages). It does not cover PECR breach reporting obligations for public electronic communications service providers (telecoms/ISPs). If a breach occurs, schools report under UK GDPR/DPA 2018, not under PECR’s CSP regime.

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (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 Information Commissioner's Office (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 Information Commissioner's Office (ICO).

  The DPO will document the decision (either way), in case it is challenged at a later date by the Information Commissioner's Office (ICO) or an individual affected by the breach. Documented decisions are stored by the DPO on the School's central systems.

  - Where the Information Commissioner's Office (ICO) must be notified, the DPO will do this via the 'report a breach' page of the Information Commissioner's Office (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 Information Commissioner's Office (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 by the DPO on the School's central systems.
- 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 other types of breach that you might want to consider could include:
    - Details of pupil premium interventions for named children being published on the school website
    - Non-anonymised pupil exam results or staff pay information being shared with governors

- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Where PECR breach reporting applies (public electronic communications services), we will meet DUAA updated PECR obligations, including the 72 hour reporting window.

Breach Recording Form

St Joan of Arc Catholic Primary School Record of Data Protection Breach
Please ensure your Head/Schools Data Protection Officer and/or Business Manager is aware. Alternatively, please contact the Information & Digital Governance team – however please do NOT delay reporting if they are not available.

Reporting on this form is on a no-blame basis

It's more important to get this reported than to get it completely right, so if there are areas that you are unsure of, please say so and submit anyway. In the case of serious breaches, you have 72 hours to report to the Information Commissioner, so this should be done without delay.

Name of Data Protection Officer: Barbara van Kan
ICO registration number:

Completed by (Name):	
Job title:	
Contact e-mail address and phone number:	
Date breach occurred:	
Date breach discovered:	

Near Miss:	☐ Yes ☐ No
Date breach reported:	
Date investigation started:	
Date investigation completed:	
Description and nature of the breach:	
Number of Data Subjects involved:	
Volume of personal data:	
Category of personal data: *List the broad types of information (e.g. name, address, health data, special category data):*	
Further details of the personal data:	
Containment Action: *Summarise actions taken to recover from the mistake, measures taken to mitigate any possible adverse effects on the individual(s) concerned and actions taken to stop it getting worse, e.g. 'collected information', or 'asked recipient to delete it'.*	
Risks as a result of the breach: *Describe the risks or consequences; for example, if the in- formation contained financial data such as bank account numbers, then there may be a risk of fraud, or if the information contained sensitive health and personal data then there may be a safeguarding issue that could leave the affected individual vulnerable.*	
Overall impact of the breach: *Consider: Sensitivity of the data; volume of data; and; potential detriment to individuals.*	

Impact of the breach on Data Subject:	
Assess who should be notified: *List and state why - informing people and organisations that have experienced an incident can be an important element in helping to manage the situation. Notifying a person whose information got misdirected, for example, would help them to take precautions against ID theft, fraud etc. Also consider if notification would serve only to worry them without any benefit; informing people about an incident is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.*	
Was the ICO notified?: *Yes/No Include date notified*	
Was the data subject informed?: *Yes/No, include rationale and date*	
Notification recommendation: *Tick all those that apply, adding additional information if required. Keep a record of the notification.*	
Evaluation: *Summarise the lessons learnt.* *Measures to be taken by the school to reduce the likelihood of such incidents from happening again:* *Consider adding to an action plan, with time for a review to check if measures have been implemented.*	
Senior staff sign off and recommendations:	The Head Teacher/Chair of Governors/DPO have read and reviewed the form and discussed the matters with relevant members of staff to reach the below conclusions: Agree/Do not agree [delete as applicable] with the assessment of risk and recommendations' The breach is not/is [delete as applicable] deemed report- able to the Information Commissioner. [Add additional points as required]
Signature:	

Name:	
Job title:	

This Policy is reviewed biennially or earlier if necessary by:

The Governing Body

It was last reviewed in

Spring 2026

It will next be reviewed in

Summer Term 2027

St Joan of Arc School
Growing together