St. John Chrysostom Federation

Data Protection Policy

Contents

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 Data Protection Act 2018 (DPA 2018), UK GDPR, and the Data (Use and Access) Act 2025 (DUAA).

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

2. Legislation and Guidance

This policy incorporates updates from the Data Protection Act 2018 (DPA 2018), UK GDPR, and the Data (Use and Access) Act 2025 (DUAA). The DUAA received Royal Assent in June 2025 and introduces new obligations that are now reflected throughout.

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.
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.

4. The Data Controller

The Federation processes personal data relating to parents, pupils, staff, governors, visitors, and others, and therefore is a data controller, with the Headteacher as the person responsible.

Each school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

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

5.1 Governors

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

5.2 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 board and, where relevant, report to the board 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 ICO.

The school has an independent data protection officer service supplied by Global Policing Limited. Global Policing is an organisation run by ex-senior police officers who specialise in working with schools and have vast experience of data protection matters. If you have any questions or comments, or wish to make any requests under the Regulations, you should contact them directly:

- Telephone (answerphone) 0161 510 2999
- Email data@globalpolicing.co.uk
- Website www.globalpolicing.co.uk/data

5.3 Executive Headteacher

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

5.4 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 Executive Headteacher 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 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 European Economic Area
- 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 DPA 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

7.1 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

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

7.2 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 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, if personal data is sufficiently anonymised, or consent has been provided

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.

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

9. Subject Access Requests and Other Rights of Individuals

9.1 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.

9.2 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request

- 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

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 unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers 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 ICO.

9.3 Recording Subject Access Requests

A record will be kept of all Subject Access Requests and logged on the SAR database. This SAR folder and database will be securely stored on site.

A file is to be created for each subject access request and in it should be the following information: -

- Copies of the correspondence between the Trust and the data subject, and between the Trust and any other parties.
- A record of any telephone conversation used to verify the identity of the data subject
- A record of the decisions and how the Trust came to those decisions
- Copies of the information sent to the data subject. For example, if the information was anonymised, keep a copy of the anonymised version that was sent to the data subject.

The file will be kept for one year and then securely destroyed.

When the request has been completed, the record of the request will be closed in the database.

9.4 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 based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the 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)

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 the Educational Record

Requests to view educational records will be dealt with as per a data access request and we will respond within 1 month of the request.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Photographs and Videos

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

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 could be used to both the parent/carer and pupil.

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.

12. Artificial Intelligence

Artificial intelligence (AI) tools are widespread and easily accessible. The school recognises both the educational potential and the data privacy risks they present.

Staff, pupils, and parents/carers must not input personal or sensitive data into generative AI tools or chatbots unless the tool has been assessed, authorised by the DPO, and subject to a data protection impact assessment (DPIA).

Under the DUAA, if personal or sensitive data is entered into an unauthorised generative AI system, this is a reportable breach. See Appendix 1 for the updated breach response.

Where the school uses AI to make decisions about individuals (e.g., in learning analytics or behaviour monitoring), the following applies:

- No fully automated decisions involving special category data will be made without explicit consent or authorisation by law.

- If an AI system is used to make a decision without human involvement, the individual has the right to request human intervention.

13. Data Protection by Design and Default

We will incorporate children's rights and protections into any new systems or processes, in line with DUAA requirements.

We will:

- Carry out DPIAs for all high-risk processing, particularly where it involves children.

- Ensure systems likely to be accessed by children comply with the Age Appropriate Design Code and DUAA obligations.

- Maintain a public record of automated processing decisions where they have a legal or significant effect on an individual.

14. Data Security and 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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 IT Acceptable Use Policy)
- 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).

15. Disposal of records

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.

16. Personal Data Breaches

We will continue to report breaches to the ICO within 72 hours where there is likely risk to individuals' rights and freedoms.

As per DUAA:

- All personal data breaches, regardless of severity, must be logged with risk assessments and remedial actions.

- Individuals must be informed promptly where there is a high risk to them, even if the breach is later resolved.

- Complaints mechanisms must be available to individuals who are dissatisfied with how a breach was handled.

See Appendix 1 for procedural detail.

17. 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.

18. Monitoring Arrangements

The DPO will monitor compliance with this policy and changes to the law, including DUAA amendments. The DPO will:

- Maintain a log of all automated processing activities.

- Ensure complaints mechanisms are in place and publicised.

- Review and revise privacy notices and training content as further DUAA guidance becomes available from the ICO.

Date Approved:	09/09/2025
Date of review:	09/09/2028
Approval : Full Governing Body	

Appendix 1: Personal Data Breach Procedure

This procedure reflects updates under the DUAA.

- All breaches, regardless of severity or whether reported to the ICO, must be documented, including likelihood and severity assessments.

- Affected individuals must be informed when the breach presents a high risk, in plain language, and with advice on steps they can take.

- A new complaints mechanism must be provided to individuals dissatisfied with how a breach was managed.

- The DPO must conduct a full review and, where necessary, present a report to the Trust Board. Persistent risks must be added to the Trust's risk register.

For further questions or to access up-to-date ICO guidance, contact:
Global Policing Limited
- Tel: 0161 510 2999
- Email: data@globalpolicing.co.uk
- Web: www.globalpolicing.co.uk/data