



Data Protection and Information Governance Policy

Policy author:	Debbie Worrall, Trust Communications, Assurance and Engagement Manager
Date approved:	Risk and Audit Committee 18 June 2026
Review period	Annual
Next review date:	Summer Term 2027

Version number.	Summary of change(s) since last version.
2.0	Re-write of previous Data Protection Policy

Data Protection and Information Governance Policy

1. Purpose

Gosforth Group (the Trust) is committed to protecting the personal data of pupils, parents and carers, staff, governors, Trustees, volunteers and other individuals it works with.

This policy sets out how the Trust complies with its legal obligations under data protection law and ensures personal data is processed lawfully, fairly, transparently and securely, in line with best practice and Trust values.

2. Legislative and Regulatory Framework

This policy is informed by, and complies with, the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012 (CCTV)
- ICO guidance and codes of practice
- Department for Education guidance

It also aligns with the Trust's Master Funding Agreement and Articles of Association.

3. Scope

This policy applies to:

- All Trust schools and central services
- All staff, Trustees, governors and volunteers
- All forms of personal data, including electronic, paper based and recorded information
- All processing activities carried out on behalf of the Trust

External organisations processing data on behalf of the Trust must comply with this policy and relevant contractual requirements.

4. Definitions

- Personal data: Information relating to an identified or identifiable living individual
- Special category data: Includes data relating to health, ethnicity, religion, biometric data, SEND and safeguarding
- Processing: Any operation performed on personal data (e.g. collection, storage, sharing, deletion)

- Data subject: The individual to whom the data relates

5. Accountability and Governance

- The Board of Trustees holds overall accountability for data protection compliance.
- The Trust acts as a Data Controller under UK GDPR.
- A Data Protection Officer (DPO) is appointed to provide independent oversight, advice and assurance.
- The DPO reports directly to the Trust Board and is involved in risk assessment and DPIAs.
- Headteachers/Principals act as day-to-day representatives of the Data Controller in their schools.

6. Data Protection Principles

Personal data must be:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Kept only for as long as necessary
6. Processed securely with appropriate safeguards

The Trust is responsible for demonstrating compliance with these principles.

7. Lawful Basis for Processing

The Trust identifies and documents a lawful basis for all processing under Article 6 UK GDPR and, where relevant, Article 9 for special category data.

The Trust primarily relies on:

- Public task
- Legal obligation

Other lawful bases (such as consent or contract) are used where appropriate and where a more suitable lawful basis does not apply.

The Trust recognises that data protection must not be a barrier to safeguarding. Personal data will be shared where necessary to protect children and vulnerable individuals, in line with statutory guidance.

8. Privacy Notices and Transparency

The Trust provides clear and accessible privacy notices to individuals explaining how their personal data is collected, used, shared and retained. These are reviewed regularly and made available via the Trust and school websites.

9. Data Subject Rights

Individuals have the right to:

- Be informed
- Access their personal data
- Rectify inaccurate data
- Erase data (where legally appropriate)
- Restrict processing
- Object to processing
- Data portability
- Protection from unlawful automated decision-making and profiling

The Trust has clear procedures in place to respond to Subject Access Requests (SARs) within statutory timescales.

10. Children and Young People's Data

The Trust recognises that children require additional protection in relation to their personal data. Where consent is relied upon, the Trust will consider the age, maturity and understanding of the child in determining whether consent should be obtained from the child or a parent/carer, in line with ICO guidance.

The Trust recognises that some children, particularly those with Special Educational Needs and Disabilities (SEND), may face additional barriers in understanding how their personal data is collected, used and shared. Privacy information will be provided in an accessible and age-appropriate manner.

The Trust also recognises that information relating to children, including photographs, video recordings and other digital content, may be misused or manipulated through emerging technologies, including artificial intelligence (AI). Appropriate safeguards will therefore be applied when collecting, storing, sharing, and publishing information relating to children.

Data protection legislation does not prevent or limit the sharing of information where there is a safeguarding concern. Where a child is at risk of harm, relevant information will be shared in accordance with statutory safeguarding guidance and the Trust's safeguarding procedures.

11. Automated Decision Making and AI

The Trust does not undertake automated decision-making or profiling with legal or significant effects.

The Trust recognises that artificial intelligence (AI) technologies present both opportunities and risks within education and children's services.

Any proposed use of AI or automated processing must comply with UK GDPR Article 22, undergo governance review and approval, include human oversight and

safeguards, align with the Trust's AI governance framework, and be subject to a DPIA where required.

The Trust recognises that AI technologies may be used to generate, manipulate or alter images, audio and video content. Such activity may present safeguarding risks, including deepfake content, AI-generated intimate images, and financially motivated sexual extortion (FMSE).

Concerns relating to AI-generated content involving children will be managed in accordance with safeguarding procedures and relevant statutory guidance.

12. Data Protection Impact Assessments (DPIAs)

A DPIA is required where processing is likely to result in a high risk to individuals, including:

- New systems or technologies
- Processing special category data at scale
- Data sharing with external organisations
- Use of AI or automated tools

All DPIAs are reviewed by the Trust Information and Assurance Lead and approved in consultation with the Trust's DPO before implementation.

The Trust maintains records of processing activities, including the purposes of processing, categories of data and the lawful basis, in accordance with Article 30 UK GDPR.

13. Data Security

The Trust applies technical and organisational security measures including role-based access controls, secure password standards, encryption, system updates, approved platforms, and cyber security monitoring.

The Trust recognises that cyber security is not solely an information governance responsibility but also an important safeguarding consideration. Cyber incidents affecting systems, services, or information relating to children may present safeguarding risks and will be managed accordingly.

14. Data Breaches

All actual or suspected data breaches must be reported immediately to the Trust Information and Assurance Lead.

The Trust:

- Maintains a breach register
- Assesses risk promptly
- Reports notifiable breaches to the ICO within 72 hours
- Notifies affected individuals where required

The Trust will review all breaches to identify lessons learned and implement improvements where required.

Failure to report breaches may result in disciplinary action.

15. International Transfers

Personal data must not be transferred outside the UK without:

- A lawful mechanism under UK GDPR
- Advice and approval from the DPO

16. Data Retention and Disposal

The Trust retains personal data only for as long as necessary and in accordance with its Records Management and Retention Policy.

Data is securely disposed of when no longer required.

17. Training and Awareness

- All staff receive data protection training
- Additional training is provided where roles involve higher risk processing
- Trustees and governors receive appropriate assurance and awareness

18. Monitoring, Review and Assurance

Compliance is monitored through:

- Periodic data protection audits
- DPIA reviews and risk assessments
- Monitoring of high-risk processing activities
- Reporting to senior leadership and the Board of Trustees

19. Specific Processing Activities

The Trust undertakes a number of processing activities that require additional safeguards, transparency and defined controls. These are governed through separate operational policies and guidance, including but not limited to:

19.1 Use of Photographs, Video and Media

The Trust recognises that images of children may be manipulated using artificial intelligence technologies, including the creation of deep-fake or AI-generated intimate images. Such activity may constitute a safeguarding concern and will be managed in accordance with the Trust's safeguarding and child protection procedures.

The Trust also recognises the safeguarding risks associated with self-generated intimate images and AI-generated imagery involving children. Where unlawful content or suspected child abuse material is identified, appropriate referrals will be considered in accordance with statutory guidance and safeguarding procedures.

Further detail is set out in the Trust's **Use of Photographs, Video and Media Policy**.

19.2 CCTV Systems

The Trust operates CCTV systems for the purposes of safeguarding, security and the prevention and detection of crime.

The Trust will ensure that:

- CCTV use is proportionate, lawful and clearly justified
- Appropriate signage is in place
- Access to footage is strictly controlled
- Retention periods are defined and adhered to
- Requests for access to footage (including SARs) are handled in line with data protection law

Further detail is set out in the Trust's **CCTV Policy**.

19.3 Telephone Call Recording

The Trust may record telephone calls for purposes including safeguarding, training, quality assurance and record keeping.

Where call recording is in place, the Trust will:

- Inform individuals that calls may be recorded
- Ensure recordings are used only for legitimate purposes
- Store recordings securely with restricted access
- Retain recordings only for a defined and proportionate period

Further detail is set out in the Trust's **Telephone Recording Policy**.

19.4 Data Sharing and Information Sharing

The Trust shares personal data with third parties where this is lawful and necessary, including with:

- Local authorities
- Safeguarding partners
- Education and support service providers

All data sharing will:

- Be supported by a clear lawful basis
- Be proportionate and limited to what is necessary
- Be subject to appropriate safeguards, including contracts or data sharing agreements

Further detail is set out in the Trust's **Data Sharing and Information Sharing Policy**.

19.5 Filtering and Monitoring

The Trust operates filtering and monitoring systems to support safeguarding, cyber security, legal compliance, and the safe use of Trust technology systems.

The operation of filtering and monitoring systems may involve the processing of personal data, including internet activity, search activity, email metadata, system usage information, and alerts generated by monitoring tools.

Such processing is undertaken in accordance with UK GDPR and the Data Protection Act 2018 and is supported by the Trust's legal obligations, public task responsibilities and legitimate interests in maintaining safe and secure educational environments.

Users will be informed of filtering and monitoring arrangements through privacy notices, acceptable use agreements and related Trust policies.

Further detail is set out in the **Trust's Filtering and Monitoring Policy**.

20. Roles and Responsibilities

- Trust Executive Team: Strategic oversight of significant, high-risk or Trust-wide safeguarding, information governance and compliance matters
- Headteachers/Principals/Corporate Leads: implementation and staff awareness concerns
- Trust Director of IT: Operational oversight of IT Systems and identification of security risks
- IT Provider: day-to-day technical support of IT Systems
- Trust Communications, Assurance and Engagement Manager: Advice, oversight and compliance monitoring
- Data Protection Officer (DPO): Independent guidance and assurance and engagement with ICO
- Designated Safeguarding Lead (DSL): receiving safeguarding concerns from the Deputy CEO(s); liaison with external agencies
- People and Culture: staff misconduct cases; employment law compliance; disciplinary support
- All Staff: compliance; reporting concerns

21. Breach of this Policy

Failure to comply with this policy may result in disciplinary action, withdrawal of access to Trust systems, termination of contractual arrangements, or other appropriate action in accordance with the Trust's disciplinary procedures and relevant policies, including safeguarding, information governance and acceptable use requirements.

22. Related Policies

This policy should be read in conjunction with:

- Acceptable Use of IT Policy
- Information Security Policy
- Safeguarding and Child Protection Policy
- Records Management and Retention Policy
- AI Position & Governance Framework
- Freedom of Information Policy
- Use of Photographs, Video and Media Policy
- CCTV Policy
- Telephone Recording Policy
- Data Sharing and Information Sharing Policy
- Filtering and Monitoring Policy
- Staff Code of Conduct
- Disciplinary Procedure

23. Contact Details

The Trust's Communication, Assurance and Engagement Manager can be contacted at:

Email: data@gosforthgroup.org.uk

Address: Gosforth Group, c/o North Gosforth Academy, Dudley Lane, Seaton Burn, NE13 6EJ

The Trust's Data Protection Officer can be contacted at:

Email: schoolsdpo@veritau.co.uk

Address: Veritau, West Offices, Station Rise, York, YO1 6GA