



Data and Information Sharing 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.
1.0	New Policy

Data and Information Sharing Policy

1. Purpose

Gosforth Group (the Trust) recognises that sharing information appropriately and lawfully is essential to supporting pupils, safeguarding individuals, delivering education services, and working effectively with partners.

This policy sets out how the Trust ensures that personal data is shared:

- Lawfully, fairly and transparently
- Safely and securely
- Proportionately and only where necessary
- In line with UK GDPR, the Data Protection Act 2018 and safeguarding requirements

2. Scope

This policy applies to:

- All Trust schools and corporate services
- All staff, Trustees, governors and volunteers
- All personal data shared internally and externally

This includes sharing with:

- Local authorities
- Safeguarding partners
- Education providers and support services
- Contractors and third-party providers
- Regulatory and statutory bodies

3. Legal and Regulatory Framework

This policy complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Education and safeguarding legislation and statutory guidance
- ICO data sharing guidance

4. Key Principles

The Trust will ensure that all data sharing is:

- Lawful, supported by a valid lawful basis
- Necessary and proportionate, limited to what is required
- Secure, shared using appropriate safeguards
- Transparent, reflected in privacy notices where appropriate
- Accountable, documented and justifiable

5. Lawful Basis for Sharing

The Trust will identify and document a lawful basis for all data sharing under Article 6 UK GDPR and, where applicable, Article 9.

The Trust typically relies on:

- Public task
- Legal obligation

Other lawful bases (such as consent) will only be used where appropriate.

6. Data Sharing and Safeguarding

The Trust recognises that:

- Data protection must not be a barrier to safeguarding
- Information will be shared without delay where necessary to protect children or vulnerable individuals

All safeguarding-related sharing will be in line with:

- Safeguarding and Child Protection Policy
- Statutory guidance

7. Routine Data Sharing

Routine data sharing includes regular or planned exchanges of information, for example:

- Census returns and statutory reporting
- Sharing with local authorities
- Partnership working with education providers
- Access to IT systems and platforms used to deliver education services

Where routine sharing occurs, the Trust will ensure:

- A clear lawful basis is established
- The scope and purpose are clearly defined
- Appropriate agreements are in place

8. One-off or Exceptional Sharing

In some circumstances, data may be shared on a one-off basis, including:

- Police requests
- Emergency situations
- Legal or regulatory enquiries

In these cases:

- Each request will be assessed individually
- Only relevant and necessary information will be shared
- Decisions will be documented where appropriate
- Advice will be sought from the Information and Assurance Lead or DPO where required

9. Data Sharing Agreements and Contracts

Where personal data is shared with external organisations, the Trust will ensure that appropriate agreements are in place where required, including:

- Data Sharing Agreements (DSAs), where two or more organisations act as data controllers
- Data Processing Agreements (DPAs), where a third-party processes data on behalf of the Trust

The Trust will ensure:

- Roles and responsibilities are clearly defined
- Security and confidentiality requirements are in place
- Data is only processed in accordance with agreed purposes

10. Minimisation and Accuracy

When sharing data, the Trust will:

- Share only the minimum necessary information
- Ensure the data is accurate and up to date
- Consider whether anonymised or pseudonymised data can be used

11. Security of Shared Data

The Trust will ensure that:

- Data is shared using secure methods (e.g. encrypted email, secure platforms)
- Access is limited to authorised individuals
- Appropriate technical and organisational safeguards are in place

Data must not be shared via:

- Personal email accounts

- Unapproved platforms or systems (for example: WhatsApp, Facebook Messenger, personal SMS/text messaging, Instagram, Snapchat, personal Google Drive or Dropbox accounts, WeTransfer, or any unapproved file-sharing websites)

12. International Data Sharing

Personal data will not be transferred outside the UK unless:

- A lawful transfer mechanism is in place
- Appropriate safeguards are applied
- Approval is sought from the Data Protection Officer

13. Record Keeping and Accountability

The Trust will maintain appropriate records of data sharing activities, including:

- The purpose of sharing
- The lawful basis
- The organisations involved

Where necessary, data sharing decisions will be documented to demonstrate compliance.

14. 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, 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

15. Breaches and Concerns

Any concerns or inappropriate data sharing must be reported immediately to:

- The Principal/Headteacher/corporate lead
- Trust Information Assurance Lead

This will be managed in line with the Trust's Data Breach procedures.

Where data sharing results in significant risk, this may be escalated to the Executive Team and, where required, reported to the ICO.

16. 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.

17. Monitoring and Review

- This policy will be reviewed annually, or earlier if there are changes in legislation
- Compliance will be monitored through audits and risk reviews
- Any incidents or concerns will inform improvements

18. Related Policies

This policy should be read in conjunction with:

- Data Protection and Information Governance Policy
- Safeguarding and Child Protection Policy
- Information Security Policy
- Use of Photographs, Video and Media Policy
- CCTV Policy
- Records Management and Retention Policy
- Staff Code of Conduct

19. Contact

The Trust Communications, 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 (DPO) can be contacted at:

Email: schoolsdpo@veritau.co.uk

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