Headteacher: Mrs Katie Smith NPQH
Website: www.glusburn.n-yorks.sch.uk
Reg Charity No 1060322
01535 632145
admin@glusburn.n-yorks.sch.uk
Colne Road, Glusburn, BD20 8PJ

GLUSBURN COMMUNITY PRIMARY AND NURSERY SCHOOL

Data Protection and Information Governance Policy

This policy was adopted by the Governing Body on	SEP 2026
This policy is scheduled for review on	SEP 2027

Introduction

"This policy is to ensure that Glusburn Community Primary School complies with the requirements of:
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Data (Use and Access) Act 2025
- The Environmental Information Regulations 2004 (EIR)
- The Freedom of Information Act 2000 (FOIA)
- Associated guidance and Codes of Practice issued under the legislation"

Scope

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

This policy is the School's main information governance policy and addresses:

- Data Protection (including rights and complaints)
- Freedom of Information
- Information Asset Management

Information security, acceptable use of systems, records management and security incident reporting will be addressed in separate policies.

Data Protection

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

The school has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to governors on the above matters

Information Asset Register

The DPO will advise the school in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

The IAR will be reviewed annually and the Head Teacher will inform the DPO of any significant changes to their information assets as soon as possible.

Information Asset Owners

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The school will ensure that IAO's are appointed based on sufficient seniority and level of responsibility.

IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

RECORDS OF PROCESSING ACTIVITIES

In addition to our Information Asset Register, we maintain Records of Processing Activities (ROPA) as required by Article 30 of UK GDPR.

Our ROPA documents:

- The name and contact details of the school (as data controller)
- The name and contact details of our Data Protection Officer
- The purposes of the processing
- A description of the categories of data subjects and personal data
- The categories of recipients to whom personal data has been or will be disclosed
- Details of transfers to third countries or international organisations
- Where possible, the envisaged time limits for erasure of different categories of data
- Where possible, a general description of the technical and organisational security measures

The ROPA is reviewed annually by the Headteacher and Data Protection Officer and is available for inspection by the Information Commissioner's Office on request.

A copy of our ROPA is available from the school office on request.

Training

The school will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

The DPO will provide the School with adequate training resources and guidance materials. The DPO will be consulted, and will offer an adequacy opinion, if the School opts to use a third party training provider.

The School will maintain a 'training schedule' which will record when employees have completed an information governance training module and when a refresher is due to be completed.

The school will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

ACCOUNTABILITY

The school is committed to demonstrating compliance with data protection law through the principle of accountability.

We demonstrate accountability by:

- Maintaining comprehensive data protection policies and procedures
- Maintaining an Information Asset Register
- Conducting Data Protection Impact Assessments for high-risk processing
- Maintaining records of processing activities
- Implementing appropriate technical and organisational security measures
- Appointing a Data Protection Officer
- Providing regular data protection training to staff
- Maintaining a data breach register
- Conducting regular audits and reviews of our data protection practices
- Documenting our decisions and the rationale behind them

The Headteacher is responsible for ensuring the school's accountability and will report to the governing body at least annually on:

- The school's data protection compliance
- Any data breaches that have occurred
- Any complaints or concerns raised
- Training completed
- Any changes to data protection law or guidance
- Any recommendations for improving our data protection practices

The governing body will review the school's data protection practices annually and will ensure that appropriate resources are allocated to data protection compliance.

Privacy notices

Glusburn Community Primary School will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. Our main privacy notice will be displayed on the school's website in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents at the start of their time at the School within their information pack.

A privacy notice for employees will be provided at commencement of their employment with the school. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).

Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

Information sharing

In order to efficiently fulfil our duty of education provision and safeguarding responsibilities, it is sometimes necessary for the school to share information with third parties.

Routine Information Sharing

Routine and regular information sharing arrangements will be documented in our main privacy notice. Examples include sharing information with:
• The Department for Education (DfE)
• The local authority
• Ofsted
• NHS health professionals
• Educational software providers
• Our multi-academy trust [delete if not applicable]

Data Sharing Agreements

Where we share personal data regularly with third parties, we will have a data sharing agreement in place that sets out:
• What data is being shared
• The legal basis for sharing
• The purpose of sharing
• Security measures in place
• Retention periods
• Responsibilities of each party

All data sharing agreements will be reviewed annually and recorded in our Information Asset Register.

Ad-hoc Information Sharing

Any ad-hoc sharing of information will be done in compliance with our legislative requirements. Before sharing information, we will consider:
• Whether we have a legal basis to share the information
• Whether the sharing is necessary and proportionate
• Whether the information is accurate and up to date
• What information needs to be shared (we will only share the minimum necessary)
• How the information will be shared securely
• Whether a data sharing agreement is needed

International Transfers

We will not transfer personal data outside the UK unless:
• We have consulted with our Data Protection Officer
• We have a legal basis for the transfer
• We have appropriate safeguards in place (e.g., standard contractual clauses, adequacy decisions)
• We have informed data subjects in our privacy notice

Safeguarding Information Sharing

Information sharing for safeguarding purposes is addressed in our Child Protection and Safeguarding Policy. We will share information where necessary to protect children from harm, in line with statutory guidance in Keeping Children Safe in Education and Working Together to Safeguard Children.

Data Protection Impact Assessments (DPIAs)

The school will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

Retention periods

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

The School has opted to adopt the retention schedule suggested by the Information and Records Management Society (IRMS).

Destruction of records

Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins.

Advice in regards to the secure destruction of electronic media will be sought from relevant IT support.

A record should be retained of all files destroyed including, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record

Third party Data Processors

All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

Relevant senior leadership may insist that any data processing by a third party ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

DATA BREACHES

What is a data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples include:
• Loss or theft of devices containing personal data (e.g., laptops, USB drives, mobile phones)
• Unauthorised access to or disclosure of personal data
• Sending personal data to the wrong recipient
• Loss of paper records containing personal data
• Ransomware or cyber attacks
• Alteration of personal data without permission

Reporting a suspected breach

All staff must report any suspected data breach immediately to:
• The Headteacher: Katie Smith
• The Data Protection Officer: [Insert DPO contact details]

Reports can be made by:
• Email: admin@glusburn.n-yorks.sch.uk
• Telephone: 01535 632145
• In person

Do not delay reporting a breach. Early reporting allows us to take swift action to minimise harm.

Our response to a breach

When a breach is reported, we will:
1. Contain the breach and limit further damage

2. Assess the severity and potential impact of the breach
3. Investigate the cause of the breach
4. Consult with our Data Protection Officer
5. Notify the Information Commissioner's Office (ICO) within 72 hours if required
6. Notify affected individuals without undue delay if required
7. Document the breach and our response
8. Review our procedures to prevent similar breaches in future

When we must notify the ICO

We must notify the ICO within 72 hours of becoming aware of a breach if it is likely to result in a risk to the rights and freedoms of individuals.

When we must notify affected individuals

We must notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

Recording breaches

All data breaches, whether or not they require notification to the ICO, will be recorded in our data breach register. This register will include:
• Date and time of the breach
• Description of the breach
• Categories and approximate number of individuals affected
• Categories and approximate number of records affected
• Likely consequences of the breach
• Measures taken to address the breach
• Whether the ICO and/or individuals were notified

The data breach register will be reviewed regularly by the Headteacher and Data Protection Officer.

For full details of our data breach procedures, see our Information Security Policy [or Data Breach Response Plan, if you have a separate document].

Access to information

Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Requests under this legislation should be made to admin@glusburn.n-yorks.sch.uk

The headteacher:

- Deciding whether the requested information is held;
- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply, and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester

FOIA requests should be made in writing. Please note that we will only consider requests which provide a valid name and address and we will not consider requests which ask us to click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.

Each request received will be acknowledged within 5 school days. The Chair of Governors and Head Teacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information; and
- Where necessary seek guidance from previous case law in deciding where the balance lies
- Consult the DPO

Reasons for disclosing or not disclosing will be reported to the next governing body.
We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.
We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied.
We will adhere to the required FOI/EIR timescales, and requests will be answered within 20 **school days.**

Requests for information under the GDPR- Subject Access Requests
Requests under this legislation should be made to admin@glusburn.n-yorks.sch.uk
Any member of staff/governor may receive a request for an individual's personal information. Whilst GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged with the school office and acknowledged within 5 days.

We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- further information for the school to be satisfied of the applicant's identity;

Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of One Calendar Month. The one calendar month timeframe begins from the date we receive a valid request (i.e., once we are satisfied of your identity and have sufficient information to respond). If we need to request additional information to verify your identity or clarify your request, the timeframe does not begin until we receive that information.

We will inform you in writing when we consider your request to be valid and when the one calendar month timeframe begins.

The school can apply a discretionary extension of up a further Two Calendar Months to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first calendar month of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information)(England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

Data Subject rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to the headteacher who will acknowledge the request and respond within One Calendar Month. Advice regarding such requests will be sought from our DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

CHILDREN'S RIGHTS

Children have the same rights as adults over their personal data. These include the rights to access their data, have it corrected or deleted, and to object to processing.

Age of Digital Consent

In the UK, children aged 13 or over can give their own consent for online services that process their personal data. For children under 13, we must obtain consent from a person with parental responsibility.

However, this does not apply to processing that is necessary for:
• The performance of a contract with the child
• Compliance with a legal obligation
• The performance of a task carried out in the public interest (e.g., education)

Exercising Rights

For pupils under 13:
• Requests to exercise data protection rights should normally be made by a person with parental responsibility
• We may accept requests directly from the child if we are satisfied they have sufficient maturity to understand the request

For pupils aged 13-18:
• We will normally accept requests directly from the pupil
• We may involve parents/carers depending on the circumstances and the child's best interests
• We will consider the child's maturity and understanding

Balancing Rights

When responding to requests from children or their parents, we will balance:
• The child's right to privacy
• The parents' right to information about their child
• The child's best interests
• The child's maturity and understanding

In cases where there is a conflict between the child's wishes and the parents' wishes, we will seek advice from our Data Protection Officer and may seek legal advice.

For more information, see our Privacy Notice for Pupils and Parents.

Complaints

Data Protection Complaints

From 19 June 2026, the Data (Use and Access) Act 2025 introduced new requirements for handling data protection complaints. These complaints have different statutory timeframes from our general complaints procedure.

What is a data protection complaint?

A data protection complaint is a complaint about how we have handled personal data.

Examples include:
- How we've responded to a subject access request
- Security measures used to protect information
- How we've collected or used personal information
- Concerns about data sharing
- Concerns about data retention or deletion
- Concerns about automated decision-making

How to make a data protection complaint

Data protection complaints should be made to:
- Our Data Protection Officer: [Insert DPO contact details]
- Or the school office: admin@glusburn.n-yorks.sch.uk or 01535 632145

Complaints can be made in writing (by post or email) or verbally (by phone or in person). We will record all verbal complaints in writing.

Our response timeframes

We will:
- Acknowledge your complaint within 30 days of receipt
- Investigate your complaint without undue delay
- Provide a substantive response as soon as reasonably practicable, and in any event within 3 months of receipt

If we need more than 3 months to investigate your complaint due to its complexity, we will:
- Inform you within 3 months of receipt
- Explain the reasons for the delay
- Provide an estimated timeframe for our response

What our response will include

Our response will:
- Explain what action we have taken (or will take) in response to your complaint
- Inform you of your right to complain to the Information Commissioner's Office (ICO) if you are dissatisfied with our response

Your right to complain to the ICO

If you are unhappy with how we have handled your data protection complaint, you have the right to complain to the Information Commissioner's Office (ICO):
- Website: www.ico.org.uk/make-a-complaint
- Telephone: 0303 123 1113
- Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

You can complain to the ICO at any time, but we encourage you to contact us first so we have the opportunity to resolve your concerns.

Other complaints

Complaints that are not about data protection (e.g., complaints about the school's educational provision, staff conduct, or other matters) will be handled through our general Complaints Procedure, which has different timeframes.

If you are unsure which procedure applies to your complaint, please contact the school office and we will advise you.

Copyright

Glusburn Community Primary School will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However it will be the enquirer's responsibility to ensure that any information provided by the school is not re-used in a way which infringes those interests, whether or not any such warning has been given.

General

The Governing body will be responsible for evaluating and reviewing this policy.