Data Protection Policy

Date adopted by governors: December 2026

Committee: Health, Safety & Safeguarding

Review date: December 2027

DATA PROTECTION POLICY

1.0 Introduction

Grasmere Academy’s Data Protection Policy has been produced to ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 (DUAA), and other associated legislation. The Policy incorporates guidance issued by the Information Commissioner's Office (ICO).

The Data (Use and Access) Act 2025 introduced amendments to UK data protection legislation. Grasmere Academy will ensure that its policies, procedures and practices reflect these changes and any subsequent guidance issued by the Information Commissioner.

The Data Protection Policy gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

Grasmere Academy is registered with the ICO as a Data Controller for the processing of living individuals’ personal information. (ICO registration number: Z3237558).

2.0 Purpose

Grasmere Academy’s Data Protection Policy has been produced to ensure its compliance with UK GDPR.

The Policy incorporates guidance from the ICO and outlines the school’s overall approach to its responsibilities and individuals’ rights under the data protection legislation.

This Policy also recognises the changes introduced by the Data (Use and Access) Act 2025 and commits Grasmere academy to implementing any additional requirements relating to children's data, data subject rights, automated decision-making, data protection complaints procedures and accountability measures.

3.0 Scope

This policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, Grasmere Academy), third parties and others who may process personal information on its behalf.

The policy also covers any staff and pupils who may be required to process or have access to personal data, for instance as part of a research project or as

part of professional practice activities. If this occurs, it is the responsibility of Grasmere Academy to ensure the data is processed in accordance with UK GDPR and that pupils and staff are advised about their responsibilities.

4.0 Data covered by the Policy

A detailed description of this definition is available from the ICO, however briefly; personal data refers to any information that identifies or could potentially identify an individual, either directly or indirectly, through one or more identifiers or characteristics. This includes both digital and physical records, and applies to data collected, stored, or processed by Grasmere Academy or by third parties acting on its behalf.

Special category data is personal data that is more sensitive in nature and requires a higher level of protection. This consists of information relating to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

5.0 The Seven Data Protection Principles

UK GDPR requires Grasmere Academy, its staff and others who process or use any personal information to comply with the seven data protection principles.

The principles require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

g) accountability, the controller shall be responsible for, and be able to demonstrate compliance with the above.

5.1 Children's Data

Grasmere Academy recognises that children merit specific protection in relation to their personal data. When processing children's personal data, Grasmere Academy will take into account the child's best interests and the higher standards of protection required by UK data protection legislation.

Where services, systems or technologies are likely to be accessed by children, Grasmere Academy will consider the potential impact on children's privacy rights and implement appropriate safeguards and protections.

6.0 Responsibilities

Grasmere Academy has an appointed Data Protection Officer to handle day-to-day issues which arise, and to provide members of the school with guidance on Data Protection issues to ensure they are aware of their obligations.

All new staff will be required to complete mandatory information governance training as part of their induction and existing staff will be required to undertake refresher training on a regular basis.

Employees of Grasmere Academy are expected to:

- Familiarise themselves and comply with the seven data protection principles.
- Ensure any possession of personal data is accurate and up to date.
- Ensure their own personal information is accurate and up to date.
- Keep personal data for no longer than is necessary, in line with retention guidelines.
- Ensure that any personal data they process is secure and in compliance with Grasmere Academy's information related policies and strategies.
- Acknowledge data subjects' rights (e.g. right of access to ***all*** their personal data held by Grasmere Academy) under UK GDPR, and comply with access to those records.

- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern Grasmere Academy.
- Ensure that any processing involving children, profiling, automated decision-making, artificial intelligence technologies or emerging digital services is assessed appropriately and, where required, subject to a Data Protection Impact Assessment (DPIA).
- Contact dpo.schools@northtyneside.gov.uk for any concerns or doubt relating to data protection to avoid any infringements of the data protection legislation.

Pupils, of Grasmere Academy are expected to:

- Comply with the seven data protection principles
- Comply with any security procedures implemented by Grasmere Academy.

7.0 Obtaining, Disclosing and Sharing

Only personal data that is necessary for a specific school related business reason should be obtained.

Pupils and their parents and or carers will be informed about how their data will be processed.

Upon acceptance of employment at Grasmere Academy, members of staff will also be informed about the processing and storage of their data which is required as part of their legal contract and employment legislation.

Data must be collected and stored in a secure manner.

Personal information must only be disclosed to third parties where there is a lawful basis to do so which means that consent is not always required

Grasmere Academy may have a duty to disclose personal information in order to comply with legal or statutory obligations. UK GDPR allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purpose and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the data protection legislation.

8.0 Retention, Security and Disposal

Those responsible for the processing and management of personal data need to ensure that the data is accurate and up to date. If an employee, student or

applicant is dissatisfied with the accuracy of their personal data, then they must inform Grasmere Academy.

Grasmere Academy staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

Grasmere Academy's retention periods, including in the Record Management Policy, define how long personal data can be retained, and where this information will be retained. These periods will differ dependant on the type of personal data, and format it is held in.

The retention periods will be set based on legislative requirements, industry practice, and in consideration of the school's lawful basis for processing the data.

The retention periods will be managed by the staff member responsible for the retention of the data, and staff will be made aware of their role in disposal and transference of personal data as applicable.

In accordance with the provisions of UK GDPR, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data held in electronic format should be deleted. Hardware or any digital storage devices should be appropriately disposed of in compliance with your ICT service provider contract and conform with UK GDPR requirements.

9.0 Safeguarding

UK GDPR does not prevent the sharing of information for the purposes of keeping children safe. The Data Protection Act 2018 allows for schools to process sensitive information without consent where there are safeguarding concerns.

If Grasmere Academy decides to share information for safeguarding purposes, the Designated Safeguarding Leads must record who they are sharing the information with and for what reason. If it is appropriate to do so, they should seek the consent of the data subject where possible. If consent is not sought, the reasons behind this decision must be recorded.

10.0 Transferring Personal Data

Any transfer of personal data must be done securely in line with Grasmere Academy's Information Security Policy.

Email communication is not always secure and sending personal data to external emails should be avoided unless it is encrypted or a password provided to the recipient by separate means.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly, and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purposes.

11.0 Automated Decision-Making and Profiling

Grasmere Academy may use information systems that incorporate automated processing or profiling functions to support educational, safeguarding, attendance, behaviour management and administrative activities. Any significant decisions affecting pupils, parents, carers or staff will not be based solely on automated processing. Where automated processing is used, the school will ensure appropriate safeguards are implemented and that meaningful human review is available where required by data protection legislation.

12.0 Data Subjects Right of Access (Subject Access Requests) Education Regs

Under data protection, individuals (both staff and pupils) have the right of access to their personal data held by Grasmere Academy. This applies to data held in both paper and electronic format, and within a relevant filing system.

Grasmere Academy shall use its discretion under UK GDPR to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.

Any individual who wishes to exercise this right should make the request in writing by contacting the Company Secretary**.**

In responding to Subject Access Requests, Grasmere Academy will undertake reasonable and proportionate searches for personal information and may seek clarification where necessary to enable an effective response. Requests will be handled in accordance with UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

Grasmere Academy will not routinely charge a fee. It will only release information upon receipt of a written request along with proof of identity or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the necessary documentation.

12.1 Data Protection Complaints

Under the Data (Use and Access) Act 2025, individuals have the right to raise complaints directly with organisations regarding the handling of their personal information.

Grasmere Academy will maintain a documented data protection complaints procedure. Any individual who believes that their personal data has not been processed in accordance with data protection legislation may submit a complaint to the school.

Complaints will be acknowledged promptly, investigated appropriately and responded to within the timescales required by the applicable legislation and guidance issued by the Information Commissioner.

Individuals remain entitled to escalate concerns to the Information Commissioner's Office where they remain dissatisfied with the school's response.

13.0 The Education (Pupil Information) (England) Regulations 2005 – Information Request

Under education regulations, those with parental responsibility can request access to a child's education record. Access to education records is a separate right and is not covered by Data Protection legislation.

An education record covers information that comes from the school, the pupil or the parent, and is processed by or for the school's governing body or teacher. This is likely to cover information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's governing body. It may also include information from the child and parent, carer or guardian.

Information provided by the parent of another child or information created by a teacher solely for their own use would not form part of a child's education record.

Those with parental authority will be able to view the record free of charge within 15 school days of the request.

If there is a request for a copy of the record, we can charge a fee for this, however, the fee will not exceed the cost of supplying the records. This will also be provided within 15 school days

14.0 Reporting a Data Security Breach

It is important Grasmere Academy responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on school systems, and unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the Data Protection Officer at dpo.schools@northtyneside.gov.uk and if it relates to an IT incident (including information security), should also be reported to the Headteacher and in certain circumstances to your ICT provider – please refer to the Data Breach reporting policy for more information.

Any breach will be investigated in line with the procedures within the UK GDPR. In accordance with that policy, Grasmere Academy will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.