Greenfields

Community Primary School, Nursery & Pre-School

Data Protection Policy

September 2026

Data Protection Policy

1. INTRODUCTION

Greenfields' Data Protection Policy has been produced to ensure compliance with the General Data Protection Regulation (GDPR) and associated legislation, and incorporates guidance from the Information Commissioner's Office (ICO).

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

Greenfields Community Primary School is registered with the ICO as a Data Controller for the processing of living individuals' personal information. (ICO registration number: **Z6953310**)

2. PURPOSE

Greenfields' Data Protection Policy has been produced to ensure its compliance with the GDPR.

The policy incorporates guidance from the ICO, and outlines the Schools overall approach to its responsibilities and individuals' rights under the GDPR.

3. SCOPE

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

The policy also covers any staff and pupils who may be involved in research or other activity that requires them 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 the school to ensure the data is processed in accordance with the GDPR and that pupils and staff are advised about their responsibilities.

4. DATA COVERED BY THE POLICY

A detailed description of this definition is available from the ICO, however briefly; personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e. as part of a relevant filing system. This includes data held manually and electronically and data compiled, stored or otherwise processed by the School, or by a third party on its behalf.

Special category data is personal data consisting 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. THE SIX DATA PROTECTION PRINCIPLES

GDPR requires Greenfields Community Primary School, its staff and others who process or use any personal information to comply with the six 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.

6. RESPONSIBILITIES

Greenfields Community Primary School 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 Greenfields Community Primary School are expected to:

- Familiarise themselves and comply with the six 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 Greenfields Community Primary School's information related policies and strategies.
- Acknowledge data subjects' rights (e.g. right of access to ***all*** their personal data held by Greenfields Community Primary School) under 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 Greenfields Community Primary School.
- Obtain consent when collecting, sharing or disclosing personal data.
- Contact dpo.schools@northtyneside.gov.uk for any concerns or doubt relating to data protection to avoid any infringements of the GDPR 2018.

Pupils, of Greenfields Community Primary School are expected to:

- Comply with the six data protection principles

- Comply with any security procedures implemented by Greenfields Community Primary School.

7. OBTAINING, DISCLOSING & 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 Greenfields Community Primary School, members of staff also consent to the processing and storage of their data.

Data must be collected and stored in a secure manner.

Personal information must not be disclosed to any third-party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, pupil or employee of Greenfields Community Primary School.

Greenfields Community Primary School may have a duty to disclose personal information in order to comply with legal or statutory obligations. 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 GDPR 2018.

8. RETENTION, SECURITY & DISPOSAL

Recipients 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 the School Business Manager.

Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with Article 5 of the General Data Protection Regulations, personal information shall be collected and retained only for business, regulatory or legal purposes.

In accordance with the provisions of the 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.

Greenfields Community Primary School staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

All departments should ensure that data is destroyed in accordance with the Retention Schedule when it is no longer required.

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, and CDs and pen drives that hold personal data passed to your I.T provider for safe disposal. Hardware

should be appropriately disposed of in compliance with your ICT service provider contract and conforms with GDPR requirements.

9. TRANSFERRING PERSONAL DATA

Any transfer of personal data must be done securely in line with Greenfields Community Primary Schools Information Security Policy.

Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with 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 into 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

10. DATA SUBJECTS RIGHT OF ACCESS (Subject Access Requests)

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

Greenfields Community Primary School shall use its discretion under 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 School Business Manager.

Greenfields 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.

11. REPORTING A DATA SECURITY BREACH

It is important that Greenfields 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 will 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 the school's 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 GDPR. Greenfields will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

12. POLICY REVIEW:

This policy will be reviewed annually. The next scheduled review is **September 2027**