DATA PROTECTION POLICY

2025 – 2027

BROOMHALL AND GRACE OWEN NURSERY SCHOOL

Data Protection Policy 2025-2027

Broomhall and Grace Owen Nursery Schools

Date of Publication	October 2025
Next Review Date	October 2027
Data Protection Office	Broomhall: Toby Wilson Grace Owen: Jordan Widison

Contents

1. Introduction

On the 25th May 2018 the Data Protection Act was replaced with the General Data Protection Regulation (GDPR).

This policy is designed to set out the ways in which personal data of staff, governors, students, parents or carers and other relevant individuals is processed fairly and lawfully.

Broomhall and Grace Owen collects and uses personal information about our staff, governors, families, pupils and other individuals that may come into contact with the school. We collect this information so that we can fulfil our educational and other associated obligations and functions. In addition to this, there may also be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Broomhall and Grace Owen is defined as a data controller and must comply with the data protection principles in its processing of personal data. This also includes the way in which data is collected, stored, used, disclosed and destroyed. We are also obliged to demonstrate compliance with the GDPR. Our failure to comply with the principles could expose the school and its staff to criminal and civil claims and possibly a financial penalty.

To view the school's purpose for holding and processing data, search for our school at https://ico.org.uk/esdwebpages/search and enter our name or ICO registration number.

Our school registration number is:

Broomhall: Z9677702
Grace Owen: Z9509885

This registration is renewed on an annual basis and updated whenever necessary.

2. Aims

Broomhall and Grace Owen aims to ensure that all personal data collected about staff, pupils, families, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions as outlined in the Data Protection Act 2018 (DPA 2018) set out in the Data Protection Bill.

That all those involved with the school community will have their data protection rights safeguarded.

Any staff member that is involved in the collection, processing or disclosure of personal data will be aware of their duties and responsibilities under this policy.

3. Scope

The policy will apply to the following:

The personal data of all staff, governors, families, students, trainee teachers or any individual carrying out duties on behalf of the school.

All personal data, whether is it in paper or electronic format.

4. Definitions

Personal Data – Any data relating to a living person who is directly or indirectly identifiable

Special Category (Sensitive) Data – Data relating to a person's race, ethnic origin, politics, religion, trade union membership, genetics, biometric, health, sex life or sexual orientation

Data Controller – The organisation which either individually or jointly decides the purposes and methods of data processing.

Data Processor – An organisation which processes data on behalf of the data controller

Processing – Just about anything which can be done with personal data

5. Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against 4 accidental loss, destruction or damage, using appropriate technical or organisational measures.

GDPR also requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Our school has processes in place for dealing with the exercise of the following rights by staff, students, governors, parents and members of the public in respect of their personal data.

- The right to be informed
- Right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Not to be subject to automated decision making or profiling

6. Privacy by Design

Under the GDPR, the school has an obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

Data Protection Impact Assessments (DPIA)

Broomhall and Grace Owen will use a DPIA to systematically analyse our processing and help us identify and minimise data protection risks by:

- Describing the processing and the purposes.
- Assess necessity and proportionality.
- Identify and assess risks to individuals.
- Identify any measures to mitigate those risks and protect our data.

A DPIA does not have to eradicate the risk but should help to minimise risks and consider whether or not they are justified.

We will conduct a DPIA for processing that is likely to be high risk.

Our school will ensure that all DPIAs include the following information:

- A description and purpose of the processing.
- An assessment of necessity and proportionality.
- Identify and assess any risks to individuals.
- Identify any measures to mitigate those risks and protect the data

Where a DPIA indicates high risk data processing, the school may consult the ICO to seek its opinion as to whether the processing of the data is GDPR compliant.

7. Data Breaches

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

The Headteacher will ensure that all school staff are aware of and understand what a data breach is. This will be part of data protection training.

When a personal data breach has occurred, the school will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then we will notify the ICO.

The school will report any notifiable breaches to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the school will inform those concerned directly and without undue delay.

The school ensures we have robust breach detection, investigation and internal reporting procedures in place. This facilitates our decision-making about whether we need to notify the ICO and the affected individuals.

When reporting a breach to the ICO we will include the following information in our report:

- The nature of the personal data breach including, where possible the categories and approximate number of individuals and records concerned.
- The name and contact details of the data protection officer (DPO).
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Failure to notify a breach when required to do so can result in a fine.

8. Data Security

It is the responsibility of all staff to ensure that the personal data that they process is stored securely and not disclosed to unauthorised third parties.

Access to personal data should only be granted to those individuals who need access for the purposes of their duties.

It will be the responsibility of the Headteacher to ensure continuity and recovery measures are in place for the security of protected data.

Electronic devices used to store personal data will be protected with a password/passcode to protect against theft or unauthorised access. The schools will also use Two Factor Authentication to ensure that devices are securely protected. Where it is technically possible, the school may also insist on the remote erasure of data from electronic devices such as phones or tablets. This includes devices owned by staff if they are using them to access personal data processed by the school.

Staff or governors are not to use their own personal devices to access personal data owned by the school.

If staff are working from home, they must have particular regard to ensure compliance with this policy and the school 'Acceptable Use ICT' policy.

Data will be destroyed securely in accordance with the Information and Records Management Society Retention Guidelines for Schools (IMRS Toolkit).

A Data Protection Impact Assessment (DPIA) will be carried out where there are new types of personal data processing that may result in a high risk to the rights and freedoms of the individual.

All staff will be aware of and follow the data breach security management process.

Please see Appendix A for a list of staff Do's and Don'ts that relate to data security.

9. Sharing Personal Data

Personal data will only be shared with third parties where we deem it to be fair and lawful to do so. If a third party is processing data on behalf of the school, we will ensure that there is a written agreement outlining the manner in which the data will be processed in accordance with the principles of the GDPR.

10. Ensuring Compliance

There will be training and guidance available to all staff.

New staff will receive data protection training as part of their induction and will be required to sign any relevant acceptable use policies.

The school will provide a Privacy notice to its workforce and parents/carers. This policy will contain the following information:

- The legal basis and purpose for data processing.
- The retention period and who the data is shared with.
- The right to request any rectifications, erasure, consent to withdraw, to complain, data portability (if applicable) and the right to know about automated decision processes.

11. Photographs

The school admissions form is revisited with families and Key Person each time child moves age groups, families can choose not to have photographs or videos used on the school website and newsletter, they agree or refuse and sign form.

This information is collated by the administrator and stored in the J drive.

12. Monitoring

The school's DPO is responsible for the monitoring and review of this policy.

This policy will be reviewed every 2 years.

13. Links with Other Policies

- Online Safety policy
- Safeguarding policies

Appendix 1

Acceptable Use Procedure 2025-2026

Broomhall and Grace Owen Nursery Schools

Written By: Natalie Cullum

I confirm that I have read and understood the Broomhall and Grace Owen Nursery Schools 'Acceptable Use' policy for Staff and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with this document.

In particular:

- Any content I post online (including outside school time) or send in a message will be professional and responsible and maintain the reputation of the school.
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents.
- If I use any form of electronic communication for contacting pupils or parents I will use the school's system, never a personal account.
- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during teaching time except in an emergency situation with the agreement of my line manager. Mobile phones should be stored out of reach and view of the children e.g. in a personal locker.
- I will never use my personal mobile phone or other personal electronic equipment to photograph or video pupils.
- Taking photographs and videos will only be done with the permission of pupils and/or their parents for agreed school activities.
- All staff are responsible for the location of their assigned iPad/laptop; this should be stored securely at the end of the day.
- Images must be downloaded on to the staff only shared area on the nurseries SharePoint.
- Under no circumstances must a camera/iPad of any kind be taken into the bathrooms without prior consultation with the Head teacher/Assistant Head teacher.
- If photographs need to be taken in a bathroom, i.e. photographs of the children washing their hands, then the Head teacher/ Assistant Head teacher must be asked first and staff be supervised whilst carrying out this kind of activity.
- I will take all reasonable steps to ensure the safety and security of school IT equipment which I take off site and should not use this for my own personal use or store any personal files on this equipment.

- I will take all reasonable steps to ensure that all personal laptops and memory devices are fully virus protected and that protection is kept up to date.

- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

- I will follow school policy on compliance with the General Data Protection Regulations (GDPR). In particular: Confidential school information, pupil information or data which I use will be stored on a device which is encrypted or protected with a strong password.

- Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended.

- I understand that I have the same obligation to protect school data when working on a computer outside school.

- I will report immediately any accidental loss of personal or sensitive information so that appropriate action can be taken.

- I understand that the school may monitor or check my use of IT equipment and electronic communications.

- I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any internet sites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.

- I will challenge any parent or visitor seen to be using a mobile phone or IT device in an inappropriate way and report this to the Head teacher/ Assistant Head teacher. I will report any concerns I have around acceptable use to the Head teacher/ Assistant Head teacher

- Staff are permitted to wear smart watches only in the event that any Bluetooth or messaging services are disabled during contact hours with children. Smart watches must not be used for calls, messaging or internet connection during contact hours with children. Any camera function on smart watches must also be disabled. Staff must not use their smart watch to process personal data, or any other confidential school information.

- I understand that by not following these rules I may be subject to the school's disciplinary procedures.

Name.....

Signed.....

Date.....