Greatham primary school

Petersfield Road, Greatham, Nr Liss, Hants. GU33 6HA
Tel: 01420 538 224
Website: www.greathamschool.co.uk
E-Mail: info@greathamschool.co.uk

HEADTEACHER: Miss J Goman

Policy Name:	**Data Protection Policy (including data breach reporting form)**
Date Adopted By Governing Body:	N/A
Signature of Chair of the Attainment Committee :	N/A
Signature of the Head Teacher	Jo Goman
Review Cycle:	3 Years
Next Review Date:	June 2017- complete January 2018 January 2021- complete January 2024- complete January 2027
Notes	

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

Greatham Primary School is the Data Controller of the personal data that it collects and receives for these purposes. Contact details for the school are as follows:

Greatham primary School, Petersfield Road, Greatham, GU33 6HA, 01420 538224

adminoffice@greatham.hants.sch.uk;

A member of the admin team is the Data Protection Officer. They may be contacted at the above address.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. **Lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner. In order for personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the UK GDPR. These include (amongst other relevant conditions) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority exercised by the school.

Where the special categories of personal data are processed, this shall include (amongst other relevant conditions) where processing is necessary for reasons of substantial public interest.

When processing personal data and special category data in the course of school business, the school will ensure that these requirements are met where relevant.

2. **Purpose limitation.** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes). The school will only process personal data for specific purposes and will notify those purposes to the data subject when it first collects the personal data or as soon as possible thereafter.

3. **Data minimisation**. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive. Personal data which is not necessary for the purpose for which it is obtained will not be collected.

4. **Accuracy.** Personal data shall be accurate and where necessary, kept up to date; Personal data should be reviewed and updated as necessary and should not be retained unless it is reasonable to assume that it is accurate. Individuals should notify the school of any changes in circumstances to enable records to be updated accordingly. The school will be responsible for ensuring that updating or records takes place where appropriate.

5. **Storage limitation.** Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The school will not keep

personal data for longer than is necessary for the purpose or purposes for which they were collected and will take reasonable steps to destroy or erase from its systems all data which is no longer required.

6. **Integrity and confidentiality**. Personal data shall be processed in a manner that ensures appropriate security of the personal data and which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection. Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller in our Data Protection Policy.
- Inform individuals of the contact details of the Data Protection Officer in our Data Protection Policy.
- Inform individuals of the purposes that personal information is being collected and the basis for this through our Privacy Notice.
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this through our Privacy Notice.
- If the school plans to transfer personal data outside the UK and the EU/EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals of their data subject rights through the Privacy Notice
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point through the Privacy Notice.
- Provide details of the length of time an individual's data will be kept through our retention schedule.
- Inform the individual and where necessary seek consent, **should** the school decide to use an individual's personal data for a different reason to that for which it was originally collected
- Check the accuracy of the information it holds and review it at regular intervals through:
    - Annual request for update to medical details
    - Annual request for update to contact details
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded as follows:
    - Personnel files stored in locked filing cabinets
    - Children's personal files stored in locked filing cabinets
    - Class information files and assessment files stored in locked cupboards

- Secure access across the HPSN2 private network which includes centrally managed firewalling, email and content filtering and Virus Protection
- Password protected computers which automatically 'lock' when not in use
- Clear desk policy at night
- Stored print on the photocopier
- Regularly changed passwords
- Restriction on memory sticks and enable all staff to remote work
- Use of work email secure line addresses only

- Ensure that personal information is not retained longer than it is needed through following the Hampshire retention schedule.
- Ensure that when information is destroyed that it is done so appropriately and securely:
  - Safe disposal of IT equipment through competent company
  - Shredding of personal information
  - Contracted waste disposal for significant quantities of personal data
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures through annual training and appropriate induction measures.

Retention and Disposal of Personal Data

- The school will dispose of personal data in a way which protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) as appropriate.
- The school maintains a Retention Schedule that is specific and relevant to the specific types of information retained. The schedule outlines the appropriate periods for retention in each case.

Complaints

In the event of a data breach such as personal data loss, report and complete a **DATA BREACH REPORTING FORM (see below) to the ICO within 72 hours** to reduce any risk of harm to the individuals affected.

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Head teacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the school admin office who will also act as the contact point for any requests for information.

DATA BREACH REPORTING FORM

The aim of this document is to ensure that, in the event of a security incident such as personal data loss, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.

The checklist can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer who can determine the implications for the school, assess whether changes are required to existing processes and notify the ICO / data subject where appropriate.

SUMMARY OF INCIDENT	
Data and time of incident	
Nature of breach (e.g. theft/ disclosed in error/ technical problems)	
Give a full description of how breach occurred	
PERSONAL DATA	
Give a full description of all the types of personal data involved with the breach but not specifically identifying the individual concerned (e.g. name, addresses, health information etc.)	
How many individuals are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further disclosed? If so, please provide details	

IMPACT OF INCIDENT	
What harm is foreseen to the individuals affected? (e.g. could the breach increase the risk of identity theft?)	
What measures have been taken to minimise the impact of the incident?	
Has the data been retrieved or deleted? If yes, state when and how	
REPORTING	
Who became aware of the breach?	
How did they become aware of the breach?	
PERSONAL DATA AFFECTED	
Give a full description of all the types of personal data involved with the breach but not specifically identifying the individual concerned (e.g. name, addresses, health information etc.)	
How many individuals are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further disclosed? If so, please provide details	