Grand Avenue Primary and Nursery School

Data Protection Policy

Compliant with Preparing for the General Data Protection Regulation

Contents

1. Rationale
2. Associated School Policies
3. Compliance / Breach
4. The Data Protection Act 2018
5. Responsibilities under DPA and Registration
6. Data Protection Principles
7. Consent for processing
8. Subject Access Rights
9. Disclosure – legal and illegal
10. Publication of school information
11. Data and Computer security
12. Secure transfer of data
13. Disposal of data
14. Training and awareness
15. Enquiries
16. Appendices
    - Definitions
    - Access request form
    - Privacy notice Parent & Carers
    - Privacy notice Staff

Agreed by staff and Governors – Spring term 2024

Next review – Spring term 2025

1. Rationale

Grand Avenue Primary and Nursery School (GAPNS) is committed to a policy of protecting the rights and privacy of individuals, including students, staff and others, in accordance with the DPA.GAPNS will process certain information about its staff, students and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- the recruitment and payment of staff
- the administration of programmes of study
- the recording of pupil progress
- agreeing awards
- collecting fees
- complying with legal obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the Data Protection Act, 2018, GAPNS will ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. Associated School Policies

This policy document needs to be read in conjunction with other school policies, including;
Safeguarding
Child Protection
e-safety and acceptable use agreement
Health and Safety
Behaviour
Staff Handbook and Code of Conduct
CCTV
Freedom of Information document
Confidentiality statement
See also Appendix A for Definitions of terms used

3. Compliance / Breach

This policy applies to all governors, staff and pupils of GAPNS. Any breach of this policy, or of the Act itself will be considered an offence and the school's disciplinary procedures may be invoked. Breaches are reported in line with ICO GDPR act 2018.

Reporting a Data Security Breach:

1. **Immediate Actions**: Any individual who becomes aware of a data security breach must immediately report it to the Data Protection Officer (DPO). The report should include details of the breach, how it was discovered, and any immediate steps taken to mitigate the impact.
2. **Assessment and Containment**: Upon notification, the DPO will assess the severity of the breach and take steps to contain it, preventing further data loss or unauthorised access.
3. **Notification to Authorities**: If the breach poses a risk to the rights and freedoms of individuals, the DPO will report it to the Information Commissioner's Office (ICO) within

72 hours of discovery. The report will include the nature of the breach, the categories and approximate number of individuals affected, and the likely consequences.

4. **Notification to Affected Individuals**: If the breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify affected individuals promptly. The notification will include the nature of the breach, the data involved, potential consequences, and steps taken to mitigate the impact.
5. **Investigation and Remediation**: The DPO will conduct a thorough investigation to determine the cause of the breach and identify necessary remedial actions to prevent recurrence. The results of the investigation will be documented.
6. **Breach Register**: All data breaches, regardless of size or impact, will be recorded in the Breach Register. This register will include details of the breach, actions taken, and lessons learned.

Best Practices for External Agencies: As a matter of best practice, other agencies and individuals working with GAPNS, who have access to personal information, will be expected to read and comply with this policy. External bodies working within the school will be required to abide by this policy.

Policy Updates: This policy will be updated as necessary, and in line with the school policy review cycle, to reflect best practices in data management, security, and control, and to ensure compliance with any changes or amendments to the DPA and other relevant legislation. GAPNS undertakes to adopt and comply with the Information Commissioner's guidance on all matters relating to Data Protection.

Data Protection Officer: The school will appoint a Data Protection Officer (Bursar) who will be responsible for data collection, processing.

4. The Data Protection Act (2018)

GAPNS policy is to abide by all statutory requirements regarding the DPA. The DPA regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children). Individuals can exercise the right to gain access to their information by means of a 'subject access request' (Appendix B). Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The DPA also sets out specific rights for school students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Student Information) (England) Regulations 2000.' For more detailed information on these Regulations see the Data Protection Guide on the ICO website.

All requests will be dealt with within one month of receipt (minus any time spent verifying identity or authorisation to act on the subject's behalf). The information will be dispatched to the subject as soon as the above process is complete

5. Responsibilities

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner, meaning that it is ultimately responsible for controlling the use and processing of the personal data.

The Head teacher is responsible for all day-to-day data protection matters, and is responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the school as well as providing training and guidance to staff on data protection best practices and conducting privacy impact assessments where necessary.

The Head teacher is also responsible for ensuring that the school's notification is kept accurate. Details of the school's notification can be found on the ICO website.
Compliance with the legislation is the responsibility of all members of the school who process personal information.
Individuals who provide personal data to the school are responsible for ensuring that the information is accurate and up-to-date.

6. Data Protection Principles

To comply with GDPR anyone processing personal data must comply with the following 8 principles.

Process personal data fairly and lawfully – All reasonable efforts will be made to ensure that individuals who are the focus of the personal data are informed of ; the identity of the data controller, the purposes of the processing, the disclosure of information to third parties, the time period for which the data will be kept, and any other relevant information.

Process data in a manner compatible with its purpose – The reason for which the data has been collected will be the only way by which the data is processed, unless the individual is informed of any additional processing before it takes place.

Ensure that data is adequate, relevant and not excessive – Personal data will not be sought which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals it will be destroyed immediately.

Personal data will be kept accurately and up to date- All data will be reviewed and updated on a regular basis. It is the responsibility of the individual giving the data to ensure it is accurate and to notify the school of any changes.

Keep personal data for as long as necessary- Personal data will only be retained for as long as it is needed, in compliance with legislation. Regular reviews will be held and a 'weeding out' process implemented. Data will be disposed of in a way that protects the rights and privacy of the individual. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required.

Process data in accordance with legislation – Data will only process personal data in accordance with individual's right. The rights of the data subject include;

- a right to be told the nature of the information the school holds and any parties to whom this may be disclosed;
- a right to prevent processing likely to cause damage or distress;

- a right to prevent processing for purposes of direct marketing;
- a right to be informed about the mechanics of any automated decision making process that will significantly affect them;
- a right not to have significant decisions that will affect them taken solely by automated process;
- a right to sue for compensation if they suffer damage by any contravention of the legislation;
- a right to take action to rectify, block, erase, or destroy inaccurate data;
- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

Ensuring that technical and organisational measures are in place against unauthorised /unlawful processing and accidental loss of data – Data will only be accessible to those who have a valid reason for accessing using it. Security measures are in place including; hard copies being kept in lockable cabinets, password protection on electronically held data, the confidential deletion/disposal of personal data, and hard drives on redundant PC's will be wiped clean before disposal.

Ensuring that personal data is not transferred to a country or territory outside the European Economic area – No data will be transferred to such territories without the explicit consent of the individual, this includes to the publication of information on the internet and school website. Any personal data collected from school website will indicate a clear privacy notice.

7. Consent for Processing

It is acknowledged that it is not always necessary to gain consent from individuals before processing their data however GAPNS will ensure that any forms used to gather data on an individual will contain a statement explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

Consent in this context is noted as; the individual has been fully informed of the intended processing and has signified their agreement (e.g. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

GAPNS will ensure that if the individual does not give consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.
Under the fair processing requirements in the DPA , the school will inform staff and parents/carers of all pupils of
-the data they hold on the staff member or pupils,
-the purposes for which the data is held
-the third parties (e.g. LA, DfE, QCA, Connexions etc.) to whom it may be passed.

A Privacy Notice will be passed to staff when they join the school and to parents/carers via the website.

The main rights for individuals are;

- *Subject access*
- *To have inaccuracies changed*
- *To have information erased*
- *To prevent direct marketing*
- *To prevent automated decision –making and profiling*
- *Data portability*

8. Subject Access Rights

The DPA extends to all data subjects a right of access to their own personal data. School policy is that:

- All requests for access must be in writing, using Access form (Appendix B) and submitted to the Headteacher.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.
- Requests from pupils will be processed and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Employees are entitlted to view their HR files
- Requests will be recorded in Subject Access log by office staff.
- Requests will be processed and a response given within 1 month.
- No charge will be made for complying for a request unless requests become frequent and excessive.

9. Disclosures

Data without explicit consent maybe disclosed in the following circumstances;

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.
- Only authorised and trained staffare allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare

officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

10. Publication of School Information

It is school policy to allow individuals to opt out of information containing personal data being published. This may include event information, staff information, pupil lists.
Staff records appertaining to individual staff will remain of a confidential nature between the Headteacher and the member of staff.
Staff and pupils using email are made aware of the DPA regarding the content of messages.
A data management statement is signed by all staff on appointment.
CCTV systems in use at GAPNS are used in a manner which complies with legislation. (See CCTV policy for further details)
Photographs of pupils are only used with permission and consent of parents/carers.

11. Data Security

GAPNS endeavours to ensure security of personal data by the following general methods

Physical Security

Building security measures are in place, for example; alarms and deadlocks. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Logical Security

- Security software is installed on all computers containing personal data.
- IT systems are set up so that the existence of protected files is hidden from unauthorised users and users are assigned a clearance that will determine which files are accessible to them.
- User names and passwords are never shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used.
- When personal data is stored on any portable computer system, USB stick or any other removable media:

1. the data will be encrypted and password protected;
2. the device will be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
3. the device will offer approved virus and malware checking software;
4. the data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

Procedural Security
In order to be given authorised access to the computer, staff will undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal. (See also Confidentiality statement and E-safety policy)

Overall security policy for data is determined by the Headteacher and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. Any queries or concerns about security of data in the school should in the first instance be referred to the Headteacher.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

12.**Secure Transfer of Data**
The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users will not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users will take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they will have secure remote access to the management information system (MIS) or learning platform.
- Users will protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care will be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (NB. to carry encrypted material is illegal in some countries)

13.**Disposal of Data**
The school will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of protected data, in either paper or electronic form, will be conducted in a way that makes reconstruction highly unlikely.
Destruction Procedures:

- **Paper Records**: All paper records containing personal data will be shredded using a cross-cut shredder or disposed of via a professional shredding service. The school

employs a company called 'Total Shred' to securely destroy personal data held on paper.

- **Electronic Records**: Electronic files will be securely overwritten using software designed for secure data deletion. Any electronic media such as hard drives, USB sticks, and CDs will be physically destroyed or wiped clean before disposal.
- **Other Media**: Any other media containing personal data, will be destroyed in a manner that ensures the data cannot be reconstructed.

14.**Training and Awareness**

All staff who handles personal data will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff;
- Staff meetings/briefings/Inset;
- Day to day support and guidance.

15.**Enquiries**

Further information about the school's Data Protection Policy is available from the school. General information about the Data Protection Act can be obtained from the Information Commissioners Office http://www.ico.gov.uk/

APPENDIX A

Definitions

Data Controller: Any individual or organisation who controls personal data, in this instance the School.

Personal Data*:* Data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

Sensitive Personal Data*:* Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.

Relevant Filing System: Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records.

Data Subject*:* An individual who is the subject of the personal data, for example, employees, pupils, claimants etc.

Processing*:* Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.

Accessible Records**:** Any records which are kept by the Organisation as part of a statutory duty, e.g. pupil records, housing tenancy records, social services records.

Parent: Has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

***Legal Disclosure*:** The release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

***Illegal disclosure*:** The release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

APPENDIX B

ACCESS TO PERSONAL DATA REQUEST (Subject Access Request – SARS)
DATA PROTECTION ACT 2018 (Section 7)

Enquirers Surname: Enquirers Forname:

Enquirers Address:

Enquirers Tel No:

Are you the person who is the subject of the records you are enquiring about (i.e the "Data Subject")? YES/NO

If
NO,_____

Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about? YES/NO

If
YES,_____

Name of child or children about whose personal data records you are enquiring:

Description of Concern/Area of Concern

Description of Information or Topic(S) Requested (In your own words)

Additional Information

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name
Address
Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 2018 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

Name of "Data Subject" (or Subject's Parent) (PRINTED)

Dated _____

APPENDIX C

Privacy Notice for Parents/Carers

GDPR 2018: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information.

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please contact:

office@grandavenue.kingston.sch.uk

We are required, by law, to pass certain information about our pupils to our local authority (LA) and the Department for Education (DfE).

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 2018.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit:
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-

database-requests-received

If you need more information about how the DfE collect and use your information, please visit:

- the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Appendix D

Privacy Notices:

The school workforce and Governors: those employed to teach, or otherwise engaged to work at, a school or a local authority

GDPR 2018: How we use your information

We process personal data relating to those we employ to work at Grand Avenue Primary School. This is for employment purposes to assist in the running of the school, the collection of data for the workforce census, and to enable individuals to be paid. The collection of this information is undertaken via the school SIMS system and HR portal; it will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority

- the Department for Education (DfE)) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- Education Personnel Management (EPM)

If you require more information about how we and the DfE store and use your personal data please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact:

- hannah.gamble@grandavenue.kingston.sch.uk

Acceptance of the terms of this notice is a condition of employment