DATA PROTECTION POLICY

DATE RATIFIED BY THE GOVERNING BODY: **4th December 2019**

DATE FOR REVIEW: **ANNUALLY**

MEMBER OF STAFF RESPONSIBLE: **HEADTEACHER**

Kenmore Park Infant and Nursery School
Data Protection Policy

The Data Protection Act 2018 and the General Data Protection Regulation (which came into effect from the 24th May 2018) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Acts. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1. Purpose

The purpose of this Data Protection Policy is to ensure Kenmore Park Infant and Nursery School and the staff working in it are aware of their obligations under the Data Protection Act 2018 and the General Data Protection Regulation (May 2018) so they comply fully with that Act.

The policy will be communicated to all staff and they will be expected to understand and abide by it.

2. Scope

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

3. The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

a) Data must be processed fairly and lawfully.

b) Personal data shall be obtained only for one or more specific and lawful purposes.

c) Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

d) Personal data shall be accurate and where necessary kept up to date.

e) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

f)Personal data shall be processed in accordance with the rights of data subjects under the 2018 Data Protection Act and General Data Protection Regulation (May 2018).

g) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

h) Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Responsibilities

Responsibility and Accountability for Data Protection is:

Headteacher who:

Has overall responsibility for ensuring that the school:

a) Manages its information and records properly and is compliant with all the relevant legislation.
b) Complies with this policy;
c) Approves procedures where personal information is processed such as: the management and communication of privacy notices; handling of requests from individuals; the collection and handling of personal information; complaints handling; management of personal information security incidents; and outsourcing and off-shoring of personal information processing.
d) The Data Protection Officer (Headteacher) will manage and address the risks to the information and will understand:

- What information is held, for how long and what purpose
- Who has access to protected data and why

The school must:

Manage and process personal data properly.
Protect the individual right to privacy.
Provide an individual with access to all personal data held on them.

The school has a legal responsibility to comply with the Act. The school, as a corporate body, is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website.

Every member of staff that holds personal information has to comply with the Act when managing that information.

5. Governors

When handling personal information on school business, governors must comply with this policy and be aware of their responsibilities as individuals under the DPA. They should be mindful that it can be a criminal offence to process personal data in a manner which they know that they are not authorised to do so. A breach of this policy by a Governor is a potential breach of the Governors Code of Conduct.

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 2018 & General Date Protection regulations May 2018.

Data protection requirements: guidance for governors

Section 13.9 of the Governance Handbook includes a section on the DPA.

It sets out certain statutory obligations placed on schools. These include:

- Notifying the Information Commissioner's Office (ICO) of the school's register entry (name and address of the data controller and a general description of how personal information is processed)
- Providing a statement or 'privacy notice' to individuals, such as pupils and parents, whose personal data is being processed or held
- Responding to requests for personal data or 'subject access requests' within 40 calendar days

It says schools should also consider:

- Obtaining their own data protection and/or legal advice
- Making sure that staff understand or follow policy when handling personal data

6. Governance and Review Responsibility

Maintaining and updating this policy belongs to the Headteacher. This policy will be reviewed every year. It will be updated as necessary to reflect best practice in data

management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998. Responsibility for monitoring adherence to this policy belongs to the school's Deputy Headteacher who should report to the Headteacher. Governors and the Headteacher will review the policy.

7. **Status of the Policy**

This policy has been approved by the Governors. All staff are expected to adhere it. Any failure to follow the policy can result in disciplinary proceedings. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Any member of staff who considers that the policy has not been followed should raise the matter with the Headteacher or the Chair of Governors if it concerns the Headteacher.

8. **Information to Parents/ Carers**

The 'Privacy Notice' In compliance with the fair processing requirements of the DPA, the purposes for which the data is held and any third parties to whom it may be passed. Parents/ Carers will be informed of the Privacy Notice at the start of every academic year in the data collection process, it is available.

9. **Sharing Information**

Within School - Before sharing personal information internally it is the responsibility of individual members of staff to ensure that they have the authority to do so and that the recipient is authorised to receive such information. Failure to do so could lead to action under the school's disciplinary procedure (and, in exceptional circumstances, in criminal charges). If there is any doubt individuals should seek the advice of the Headteacher. In emails staff should aim to use student initials and year group as identification in subject box. They should send personal information only to relevant subject and pastoral staff.

Externally - There are occasional instances where information is shared with partners or outside organisations through agreement. Each agreement, as a minimum, must clearly state the information that will be shared, the purposes for sharing, the basis on which sharing is carried out and the responsibilities for handling and maintaining the personal data.

10. External Disclosure Requests

Requests from external organisations or third parties for personal information about individuals should be passed to the Headteacher. Under no circumstances should any personal information about any individual be passed outside the school without the authority of the Headteacher. Requesters would have to put any request in writing and send it to the Headteacher.

11. **Subject Consent**

On occasion individuals give consent for the processing of their personal information. Staff must ensure that any consent given for the processing of personal information is

fully informed and freely given and that individuals are aware that they may withdraw consent at any time and what the consequences would be if they withdrew their consent. It is advisable not to rely on consent for the processing of personal data if there is another legitimate criterion for processing which could be applied. Before relying on consent, service areas must consider the impact on the service should individuals refuse or withdraw consent. If it is deemed that the consent of individuals is necessary, staff should be aware that, in the case of sensitive personal data, individuals have to give explicit consent to the processing. It is therefore good practice to obtain written consent in such cases and the school will aim to do this.

12. Data Subjects Rights

The school will ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include the right:

- to be informed that processing is being undertaken;
- of access to one's personal information;
- to prevent processing in certain circumstances; and
- to correct, rectify, block or erase information which is regarded as wrong information.

13. **Retention and Disposal of Data**

It is the responsibility of the individual service areas holding personal information to ensure that the information that they hold is kept accurate and up-to-date and is not held for any longer than is necessary for the purpose for which it was collected. When the data is no longer required the service area must dispose of the data safely. Usually we keep student documentation / staff files for 7 years (unless otherwise specified) following leaving the school. Advice on determining retention periods and disposing of data can be obtained from the Information and Records Management Society. Data is held securely both on and off site. (refer to the Retention Policy and Retention schedule guidance).

14. **Publication of Personal Data**

Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasion it may be appropriate to publish personal information with the individual's consent. However, in such cases staff must ensure that the consent is fully informed and freely given. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately. Staff should be aware that publishing personal information on the school's web pages or internet effectively means that the information is published world-wide and outside the EEA. It, therefore, cannot be protected by the DPA or the European Directive on Personal Privacy. Great care should be taken before publishing personal information (or any information from which individuals could be identified) in this manner and the approval of the Headteacher should be obtained before publication of information, beyond that of student name and year group. The school newsletter is checked for suitability by the Headteacher.

15. **Medical Records**

These are classed as sensitive personal data under the DPA and, therefore, additional care should be taken when processing this information. In particular, before disclosing the medical records of anyone as part of a Subject Access Request, the advice of the relevant medical practitioner and the Headteacher must be sought as to whether the information should be released or not.

16. **Staff Records and the Monitoring of Staff**

The school will comply with the ICO's employment practices code in relation to the processing of staff personal information. This Code exemplifies good practice and strikes a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. In particular, staff monitoring should only be carried out in accordance with this code of practice.

17. **Sensitive and High Risk Personal Data**

Sensitive personal data is defined in the DPA as information concerning an individual's: racial or ethnic origin political opinions religious beliefs or other beliefs of a similar nature trade union membership physical or mental health or condition sexual life criminal convictions or alleged offences Extra care must be taken when processing sensitive personal data as additional requirements under the DPA must be met to ensure that the processing is legitimate and safe. The advice of the Headteacher should be sought before any new processing of sensitive personal data commences. There is also some personal information which is regarded as high risk and therefore a risk assessment should be carried out and additional security precautions should be implemented before processing such information. High risk personal information includes, but is not limited to:

- personal bank account and other financial information;
- national identifiers, such as national insurance numbers;
- personal information relating to vulnerable adults and children;
- detailed profiles of individuals;
- sensitive negotiations which could adversely affect individuals; and
- large numbers of records containing personal information.

18. **Personal Data Held**

The school will maintain an inventory of all the categories of personal information that it holds and the reasons for holding that data. Such inventories will be reviewed and updated at least annually and any changes communicated to the Data Protection Officer as soon as they are made so that the school's notification may be kept up-to-date. The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records.

Personal data is defined as any combination of items that identifies an individual and provides specific information about them, their families or circumstances.

This will include:

a) Personal information about members of the school community- including students, members of staff and parents/carers: names, addresses, contact details, legal guardianship contact details, health records, disciplinary records etc.
b) Curricular data; class lists, student progress records and reports.
c) Professional records; employment history, taxation and national insurance records, appraisal records and references.
d) Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members. 5.2 Security of Personal Data The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:
e) any personal data which they hold is kept securely; and
f) personal information is not disclosed either orally, in writing, electronically or otherwise to any unauthorised person. Personal information should be: if hard copy:
g) not left accessible to unauthorised persons;
h) preferably and where possible, kept in a locked filing cabinet or in a locked drawer; and
i) disposed of as confidential waste. if electronic:
j) be password protected or kept only on portable media which is itself secure in accordance with the school's policy.
k) Where practicable, held on a PC with 'time out' facility and/or where SIMS is closed down daily.
l) be deleted in accordance with corporate retention periods and evidence of such deletion recorded to provide for necessary audit trails.
m) Passwords to be enforced strong passwords at least eight characters long and a 90 day prompt to change passwords (by Sept)
n) Every electronic system that holds personal information has a designated manager who has overall responsible for controlling access to and the information security of that system, this being the school 'Network Manager' Advice on making personal data secure is provided by the Data Protection Officer.

Any incidents where personal data has been lost or disclosed to unauthorised recipients should be immediately reported to the Headteacher who will advise what action should be taken to mitigate the damage.

19. **External Data Processing**

All contracts with third-party providers, where the processing of personal data is required, shall include a requirement for the contractor to comply with the requirements of the Data Protection Act 2018 and General Data Protection Regulations May 2018.

20. **CCTV monitoring**

CCTV monitoring must only be carried out in accordance with the ICO's code of practice on CCTV.

21. **Information Commissioners Office (ICO)**

The ICO also provides guidance specifically for schools. The webpage includes information on:

- Lesson plans
- Biometrics
- Publishing exam results
- Taking photos in schools
- Allowing the use of personal devices
- Cloud computing