Data Protection Policy

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions including GDPR.

The Head Teacher and Governors of Epinay School intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data is aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the school's Data Protection Policy is available from the Head Teacher. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (www.dataprotection.gov.uk).

Fair obtaining and processing

The school undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purpose of for which the data is held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting the data will explain the issues before obtaining the information.

"Processing" means obtaining, recording or holding the information or data or carrying out any of set of operations on the information or data. "Data subject" means an individual who is the subject of personal data or the person to whom the information relates. "Personal data" means 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, if published in the press, internet or media. "Parent" has a meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child.

Data integrity

The school undertakes to ensure data integrity.

Data Accuracy

Data held will be as accurate and up to date as is reasonable possible. If a data subject informs the school of a change of circumstances, their computer record will be updated as soon as is practicable. A printout of their data subjects every 12 months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate or “challenged”. In the case of any dispute, we will try to resolve the issue informally but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage either side may seek independent arbitration. Until resolved, the “challenged” maker will remain on all disclosures of the affected information and the information will contain both versions of the information.

Data adequacy and relevance

Data held about people will be adequate, relevant and not excessive in relation to the purposes for which the data is being held. In order to ensure compliance with this principle, the school will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of time

Data held about individuals will not be kept for longer than necessary for the purposes of registered. It is the duty of the Head Teacher to ensure that obsolete data is properly erased.

Subject areas

All data subjects have a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

Requests from students will be processed as a subject access requested and the copy will be given directly to the student unless it is clear that the student does not understand the nature of the request.
Requests from students who do not appear to understand the nature of the request will be referred to parents/carers.
Requests from parents/carers in respect of their own child will be processed as requests made on behalf of the subject data (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing subject access requests

See Subject Access Request Policy.

Authorised disclosures

The school will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the school’s authorised officer may need to disclose data without explicit consent for that occasion.

The circumstances are strictly limited to:
Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.

- Student data disclosed to authorise recipients in respect of their child’s health, safety and welfare.

- Student 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 (eg 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 local authority are IT liaison/data processing officers, for example in the local authority, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by staff 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 students' 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 are, or have been, either the subject of or at risk of child abuse.

A legal disclosure is the release of information from the computer to someone who requires the information to do their job within or for the school, provided that the purpose of that information has been registered.

An illegal disclosure is 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.

Data and computer security

The school undertakes to ensure security of personal data by the following general methods.

Physical security

Appropriate building security measures are in place. Only authorised persons are allowed in the server room. Data is securely stored when not in use. Visitors of the school are required to sign in and wear identification badges whilst in the school and are, where appropriate, accompanied.

Logical security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up regularly.

Procedural security

In order to be given authorised access to the computer, staff will have to undergo checks. Staff are aware of data protection obligations. All confidential documents are shredded before disposal.

Overall security for data is determined by the Head Teacher and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Individual members of staff can be personally liable 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 a disciplinary matter and serious breaches could lead to dismissal.

Policy approved by Governors:	January 2026
Date of next review by Governors:	January 2027