Abacus Primary School
Data Protection Policy

The School recognises its role and responsibilities as both a data controller and processor. Personal data is information that relates to an identifiable living individual that is processed as data. In addition, sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical and mental health, sexuality and criminal offences.

The person with overall responsibility for Data protection is the Headteacher, supported by the office manager (Elaine Jones) and a named governor (John Wood). In line with GDPR the school has appointed a Data Protection Officer (DPO) whose role is to ensure compliance.

Aims & Objectives:
The aim of this policy is to provide a set of guidelines to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data

The objective of the policy is to ensure that the school acts within the requirements of the General Data Protection Regulation (GDPR) 2018.

Fair Obtaining
The School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for the collection of the data, the purposes for which the data is held, the likely recipients of the data and their right to access that data; either under the Education (Pupil Information) (England) Regulations 2005 or GDPR 2018. Data subjects will be informed about the collection and use of their data through the use of Privacy Notices.
As well as receiving a copy of the Privacy Notice on admission of child or induction of new staff, a copy is available on the school website.

Data Integrity
The school undertakes to ensure data integrity by the following methods:
Data Accuracy – data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances, their records will be updated as soon as is practicable.
Anyone has the right to question and correct inaccurate information, but this must be matters of fact, not opinions.
Data Relevance – data held about people will be relevant to the purpose for holding the data. The data held will not be excessive in relation to the purpose for which it was

collected. In order to ensure compliance with this principle the school assets register will identify how data is used, stored, transferred (as relevant) and disposed of.
Length of Time – data held about individuals will not be kept for longer than is necessary for the purposes for which it is held. (See Scheme of Retention)
It is the duty of the DPO to ensure that the data disposal systems are adhered to.

Subject Access Requests
Under the Data Protection Act 1998, and other regulating acts, all data subjects have the right to access their personal data. Personal data should always be of direct relevance to the person requesting the information. A document discussing more general concerns may not be defined as personal data.

1. A child can request access to his/her own data. The request is not charged and does not have to be in writing. Staff will judge whether the request is in the child's best interests, and that the child will understand the information provided. They may also wish to consider whether the request has been made under coercion. If they determine that either the child will not understand or it is not in their best interests, the request will be referred to the child's parents.

2. A parent can request access to or a copy of their child's school records and personal data. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be a charge for photocopying records.

Staff should check, if a request for information is made by a parent, that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force and that there is sufficient proof of identity.
For educational records access must be provided within 15 school days and all other records no later than 40 days.
3. A member of staff can request access to their own records, there is no charge for access or copies.

All requests will be acknowledged in writing on receipt, and access to records will be arranged as soon as possible. If third party consents are required, the school will arrange access to those documents already available, and notify the individual that other documents may be made available later or provide the information in a redacted form.
The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.) This will enable staff to deal with a complaint if one is made in relation to the request.

Authorised Disclosures

- In general, the School will only disclose data about individuals with their consent. However, there are circumstances under which it is necessary for the

school's authorised officer(s) to disclose data the without express consent of the data subject.

- These circumstances are limited to:
- Pupil data disclosed to authorised recipients in respect of education and administration necessary for the school to perform its legitimate duties and obligations.
- Pupil data disclosed to authorised recipients in respect of a pupil's health, safety and welfare.
- Staff data disclosed to the relevant authority in respect of payroll and school's staff administration

Only authorised and properly instructed staff are permitted to make external disclosures of personal data. Data used within the school is only made available if the staff member needs to know the information for their work within the school.

Data Security

The School undertakes to ensure security of personal data by the following general methods –

- Physical Security - Appropriate building security measures are in place, such as alarms and lockable cabinets. Only authorised persons have access to the physical server in the computer room. Visitors to the school are required to sign in and out 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. In addition, all laptops and staff memory sticks are encrypted. Computer files are backed up and stored in the lockable fire cabinet.
- Procedural Security - All staff are trained and instructed in their Data Protection obligations and their knowledge updated as necessary. Documents containing personal data are either shredded or disposed through a confidential documents disposal company. The school Data Assets Register details how documents should be stored, used and safely disposed of.

Data Breaches

- The above measures are in place to avoid any data breaches however in the event of a breach the school will take the following actions
- Report any data breach to the Information Commissioner's Office (ICO), where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.
- Report any breach to the Governing Body
- Investigate the circumstances and determine any new or additional security measures that need to be implemented e.g. additional training.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the School will also notify those concerned directly.
Any deliberate breach of this Data Protection policy will be treated as a disciplinary matter and serious breaches of the Act may lead to dismissal.

Reviewing:
This policy will be reviewed by the Resources Committee annually.