ALAMEDA MIDDLE SCHOOL

INSPIRE • ACHIEVE • EXCEL

DATA PROTECTION POLICY GDPR V1

DOCUMENT STATUS

ORIGINAL AUTHOR	Maxine Warner
DATE OF PRODUCTION	May 2018
CURRENT STATUS	Approved
REVIEWING BODY	Full Governing Body
REVIEWED ON	September 2018
DATE FOR NEXT REVIEW	September 2021
RELATED POLICIES (IF ANY)	Freedom of Information Publication Scheme

TABLE OF CONTENTS

DOCUMENT STATUS I

TABLE OF CONTENTS II

1. INTRODUCTION 1

2. DEFINITIONS 2

3. THE DATA CONTROLLER 3

4. THE PROCESSING OF PERSONAL DATA 3

5. DATA PROTECTION PRINCIPLES 3

6. ROLES AND RESPONSIBILITIES 4

7. PRIVACY NOTICE 5

8. SUBJECT ACCESS REQUESTS 5

9. STORAGE OF RECORDS 7

10. DISPOSAL OF RECORDS 7

11. TRAINING 8

12. DATA BREACHES 8

13. MONITORING ARRANGEMENTS 9

1. INTRODUCTION

The school aims to ensure that all Personal Data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulation which came into force on 25th May 2018.

This policy applies to all data, regardless of whether it is in paper or electronic format.

- This policy meets the requirements of the General Data Protection Regulations (GDPR), and is based on Guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.
- In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.
- This policy complies with our Funding Agreement and Articles of Association which are published on the school web site.

2. DEFINITIONS

TERM	DEFINITION
Personal Data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Special Categories of Data	Data such as: • race; • ethnic origin; • politics; • religion; • trade union membership; • genetics; • biometrics (where used for ID purposes); • health; • sex life; or • sexual orientation.
Processing	Obtaining, recording or holding data
Data Subject	The person whose Personal Data is held or Processed
Data Controller	A person or organisation that determines the purposes for which, and the manner in which, Personal Data is Processed
Data Processor	A person, other than an employee of the Data Controller, who Processes the Personal Data on behalf of the Data Controller
Data Protection Officer	The school has appointed a Data Protection Officer (DPO) as it is a public body. The DPO will assist the school in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for Data Subjects and the Supervisory Authority.

3. THE DATA CONTROLLER

The school processes Personal Data relating to pupils, staff and visitors, and, therefore, is a Data Controller. The school assigns responsibility of Data Controller to the Business Manager The school is registered as a Data Controller with the Information Commissioner's Office and renews this registration annually.

4. THE PROCESSING OF PERSONAL DATA

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

5. DATA PROTECTION PRINCIPLES

So far as is reasonably practicable, the school will comply with the principles of Article 5 of the GDPR to ensure all data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified within a reasonable timescale;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5 (2) requires that:

- "the Data Controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The school has developed this policy to ensure, as far as possible, that this requirement is met.

6. ROLES AND RESPONSIBILITIES

- The Governing Body has overall responsibility for ensuring that the school complies with its obligations under the GDPR.
- Day-to-day responsibilities rest with the Headteacher, or the Deputy Headteachers in the Headteacher's absence. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or Processing of Personal Data.
- Staff are responsible for ensuring that they collect and store any Personal Data in accordance with this policy. Staff must also inform the school of any changes to their Personal Data, such as a change of address.
- The school will undertake regular data audits to ensure that Personal Data is stored in accordance with the GDPR.

- The school will undertake a Data Protection Impact Assessment on any new processing procedures from 25th May 2018

7. PRIVACY NOTICE

The school will issue pupils and parents and staff separate Privacy Notices that include the following.

- Identity and contact details of the Data Controller and where applicable, the controller's representative) and the Data Protection Officer
- Purpose of the processing and the legal basis for the processing
- The legitimate interests of the Controller or third party, where applicable
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data

These will be published on our school web site.

8. SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. Contact details are written on the Privacy Notices. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9. STORAGE OF RECORDS

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

10. DISPOSAL OF RECORDS

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

The school will create a detailed retention policy in line with GDPR and Department for Education guidelines.

11. TRAINING

Our staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

12. DATA BREACHES

A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. It also means that a breach is more than just about losing Personal Data.

Personal Data breaches may include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a Data Controller or Data Processor;
- sending Personal Data to an unauthorised recipient;
- devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

When a breach is identified, there is an obligation for the Data Processor to notify the Data Controller.

The Data Processor will notify the Data Controller of any breach or suspected breach without undue delay.

There is an obligation for the Data Controller to notify the Supervisory Authority within seventy two (72) hours of the breach or suspected breach being identified.

- The data controller will notify the Supervisory Authority under GDPR if it is likely to result in a risk to people's rights and freedoms. This decision should be taken in consultation between the Headteacher and the Data Protection Officer.
- The notification should contain:
- A description of the nature of the breach
- Categories of personal data affected by the breach
- Approximate numbers of records and data subjects affected
- The possible consequences of the breach
- A description of measures already taken and to be taken to mitigate the breach
- Communicate details of the Data Protection Officer

- There is no requirement to notify if unlikely to result in a risk to the rights and freedoms of natural persons (Article 33, clause 1)
- If the school fails to report within 72 hours this must be explained to the ICO
- The school must document personal data breaches, effects and remedial action. This will enable assessment of compliance with these requirements.

In the event of an actual breach there are obligations for the Data Controller to communicate a Personal Data breach to the affected Data Subjects

- The school must communicate to the Data Subject(s) without undue delay if a high risk. The decision to communicate should be taken in consultation with the Headteacher and the Data Protection Officer.
- Communication will be in clear plain language
- The Supervisory Authority may compel communication with affected Data Subjects although exemptions apply if:
  - appropriate technical and organisational measures have been taken; and
  - a high risk to data subject will not materialise; or
  - communication with the Data Subject would involve disproportionate effort

13. MONITORING ARRANGEMENTS

The Business Manager is responsible for monitoring and reviewing this policy.

The Headteacher ensures that the school complies with this policy.

This document will be reviewed when the General Data Protection Regulation comes into force, and then every 3 years or as required by legislative change.

Review of school records every 3 years.

At every review, the policy will be shared with and approved by the governing body.