DATE PALM
PRIMARY
Building foundations for life

GDPR (DATA PROTECTION) POLICY

DATE PALM STATEMENT of INTENT

At Date Palm our vision is for the School to ensure our pupils grow like a Date Palm tree – with **strong foundations, lofty branches and produce fresh fruit**:

- ✓ To build **Strong Foundations for Character Development** that:
  Instil values; inspire each pupil; display best manners.
- ✓ To have **Lofty Branches of Educational Excellence** that will:
  Provide a broad and varied range of experiences and learning opportunities; help each pupil progress and develop in all aspects; support their skills and talents.
- ✓ To produce **Fresh Fruit that provides services to their Communities** in order to:
  Become responsible and confident citizens; make a positive difference; commit to charitable endeavours; become effective contributors towards Britain's future.

Reviewed by	Position	Signature
Saira Karim	Assistant Head	S.Karim
Sabina Yesmin	Safeguarding Governor	S.Yesmin
Kamrul Islam	Data Protection Officer	K.Islam

Reviewed: February 2024
Next review date: February 2025

DATE PALM
PRIMARY
Building foundations for life

GDPR (DATA PROTECTION) POLICY

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

Date Palm Primary School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Date Palm Primary School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998, and changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

Date Palm Primary School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this GDPR Policy.

The legal bases for processing data are as follows –

a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

c) Legal obligation: the processing is necessary for the school to comply with the law

The school is also committed to ensuring that members of staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings. Governors are ultimately responsible for implementation; however, the Designated Data Controllers will deal with day-to-day matters.

The School has two Designated Data Controllers: They are the Head Teacher and Deputy Head Teacher. The Data Protection Officer (DPO) is the Chair of Directors, who will overlook the implementation of this policy.

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

Notification

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

Fair Processing / Privacy Notice

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff and parents prior to the processing of an individual's data.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection laws and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently.

The School cannot be held responsible for any errors unless the staff member has informed the School of such changes. If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in this policy.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on removable storage media, that media must itself be encrypted.

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Security of data shall be achieved through the implementation of physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

Rights to access Information

All staff, parents and other users are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the school is doing to comply with its obligations under the 1998 Act & 2018 Regulation.

To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will

state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right to access certain personal data being kept about them or their child either on computers or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the Designated Data Controller. The school will not charge to process this request.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

Other schools

- If a pupil transfers to another school, their academic records and other data that relates to their behaviour, health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Examination authorities

- This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities

- As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts

- If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Social workers and support agencies

- In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Right to be Forgotten:

- Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school.

Subject Consent

In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The School has a duty of care to all staff and students and must therefore make sure those employees and those who use School facilities do not pose a threat or danger to other users. The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Retention of data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

The school will not keep personal data on pupils for any longer than is necessary. Information such as statistical data, and information that is collected to be kept as part of school records, will be kept by the school even after the child leaves.

It is very important that all examination results, certificates and records indicating the progress of a student are safely kept by their parents/carers as the school cannot guarantee that this information will be kept indefinitely by the school.

Our document retention periods are in line with London Borough of Tower Hamlets policy & guidance issued by the Information & Records Management Society. A summary of the retention periods for the main types of documentation we hold is detailed below.

Pupil Records: Retained for the period that the child attends the school and then transferred in full to the next school. The last school attended by the child must keep the records for 7 years from the child's 18th birthday (25 years of age).

- Child Protection records – 35 years.
- Statement of Special Educational Needs – 35 years.
- Advice & information regarding educational needs -12 years following closure of the file
- Attendance Registers - 3 years from date of register
- Admissions – 25 years
- Pupils' work – 2 years

Governing Body Documents:

- Minutes, reports, complaints - 6 years from the date of the meeting, report or resolution of the complaint
- School Development Plans - 7 years

HR Documents:

- Personal files – 7 years
- Interview notes & recruitment records – 1 year
- Warnings – oral, 6 months ; first written, 6 months ; second written, 1 year ; final warning 18 months.

Health & Safety:

- Accident reports – 7 years (adults), DOB +25 years (pupils)
- Risk Assessments – 4 years
- Fire Log Book – 7 years
- Risk Assessments for trips & visits - 14 years

Administrative Documents

- Inventories – 7 years

- Prospectus – 3 years
- Newsletters/circulars – 2 years
- Visitors book – 3 years

Finance Documents

- All documentation – 7 years

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Equality Policy. Because this information is considered sensitive, staff (and students where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

Photographs and videos

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data

Hard copy data, records, and personal information are stored in locked cupboards. The only exception to this is medical information that may require immediate access during the school day. This will be visibly displayed in each classroom.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- If USBs contain sensitive data, the USB must be encrypted and sensitive data should be placed in a secure vault
- Paper-based data should be stored securely where unauthorised people are unable to access it
- Documents with personal data should be removed immediately from communal areas such as printers
- Personal data should be disposed of securely e.g. shredder
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended
- Sensitive information should not be viewed on public computers
- Encrypted email services should be used when emailing sensitive information

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All paper-based data will be disposed of by using a shredder.
All electronic data will be passed to a disposal partner with demonstrable competence in providing secure disposal services.

Conclusion

Compliance with the 1998 Act and 2018 Regulation is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.