King's Oak Primary School

Data Protection Policy May 2018v1

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

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.

Introduction

King's Oak Primary School is required to retain information regarding its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example.

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, King's Oak Primary School must comply with the Data Protection Principles which are set out in the General Data Protection Regulation. In summary under article 5 these state that personal 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 without delay;
- 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 controller shall be responsible for, and be able to demonstrate, compliance with the principles."

King's Oak 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 Data Protection Policy.

On what basis do we collect and handle personal data?

We collect and process pupil information under Article 6 and Article 9 of the European General Data Protection Regulation from 25 May 2018. Under Article 6(1)(e) our lawful basis for processing data is that it is a Public task and the processing is necessary for us to perform a task in the public interest. Under Article 9(2)(g) our lawful basis for processing sensitive data is that processing is necessary for reasons of substantial public interest. We also collect and use data under section 537A of the Education Act 1996 and section 83 of the Children's Act 1989.

We collect and process staff data under Article 6 and Article 9 of the European General Data Protection Regulation from 25 May 2018. Under Article 6(1)(e) our lawful basis for processing data is that it is a Public task and the processing is necessary for us to perform a task in the public interest. Under Article 9(2)(g) our lawful basis for processing sensitive data is that processing is necessary for reasons of substantial public interest. We also collect your data in line with section 114 of the Education Act 2005.

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Privacy Notice

The school will issue pupils and parents and staff privacy notices that includes the following.

- Identity and contact details of the 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

The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the GDPR, and the Governors are therefore ultimately responsible for implementation.

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, who would be:
The Headteacher

Data Protection Officer

The school will appoint a Data Protection Officer as it is a public body. The DPO will assist the school in monitoring internal compliance, inform and advise on our data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

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 pupil's work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the Data Protection Policy to remain confidential.

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 a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

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 GDPR.

All staff, parents and other users have a right under the GDPR to access certain personal data being kept about them or their child either on computer 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 aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month as is required under GDPR.

The school may take legal advice in determining what information may be released. Certain data is exempt from the right of access under the GDPR, and this may include:

- Information that identifies other individuals,
- Information that the School or College reasonably believes is likely to cause damage or distress,
- Information that is subject to legal professional privilege,

Certain data is exempted from the provisions of the GDPR. Information relating to the following will not be released to individuals:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the school.

The above are examples only of some of the exemptions under the Regulation. Parents and students should note that any information relating to child protection, or which reveals the identity of another student, will not be released.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the school can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where the school refuses to respond to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

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 Sick Pay Policy or the Equal Opportunities Policy.

Because this information is considered **sensitive** under the GDPR, staff (and pupils 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.

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 pupil 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. A retention schedule will be developed at the school.

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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Personal data breaches can include:

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

Obligation for data processor to notify data controller

- The data processor will notify the data controller without undue delay after becoming aware of the breach.

Obligation for data controller to notify the supervisory authority

- The data controller will notify the supervisory authority under GDPR if it's likely to result in a risk to people's rights and freedoms. This decision should be taken in consultation with the Executive Principal and the Data Protection Officer.
- Notification to the ICO to be made without undue delay and not later than 72 hours.
- Description of the nature of the breach
    - Categories of data
    - Approximate numbers of records and data subjects affected

- Describe likely consequences
- Describe measures taken – or 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.

Obligation for data controller to communicate a personal data breach to data subjects

- The school must communicate to the data subject without undue delay if a high risk. The decision to communicate should be taken in consultation with the Executive Principal and the Data Protection Officer.
- Communication will be in clear plain language
- The supervisory authority may compel communication with data subject
- Exemptions if:
    - appropriate technical and organisational measures taken
    - high risk to data subject will not materialise
    - communication with data subject would involve disproportionate effort

Conclusion

Compliance with the GDPR 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.