Keresforth Primary School

Data Protection Policy

Reviewed March 26
Date of next review – March 27

Approved by _____ Date _____

Chair of Finance Committee

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.

1. Introduction

Keresforth 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, Keresforth Primary School so far as is reasonably practicable, comply with the Data Protection Principles which are set out in theUK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

In summary these state that personal data shall:

1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant and not excessive for that purpose.
4. Be accurate and kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the data subject's rights.
7. Be kept safe from unauthorised access, accidental loss or destruction.
8. Be stored only in countries within the EU or with companies that comply with the EU's Data Protection Directive (e.g. The Safe Harbour Scheme).

Keresforth 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.

2. 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.

3. The Data Controller and the Designated Data Controllers

The School as a body is the Data Controller under the 2018 Act, and the Governors are therefore 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 Headteacher and the

Business Manager.
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 in writing with the appropriate Designated Data Controller, who would be the Business Manager
School has a Data Protection Officer to provide support with SAR's and data breaches in addition to training.

4. Responsibilities of School

The school is responsible for:

1. Renewing the annual Data Protection Notification Policy with the Information Commissioners' Office and Displaying the Keresforth Primary Freedom of Information Publication Scheme on school notice boards.
2. Ensuring that all information on pupils and their families is accurate and up to date.
3. Ensuring parents are aware of the Privacy Notice – Data Protection Act 2018 -which explains what data is held about their children and how they may request this information.
4. Defining the level of access that staff have to access confidential information stored on the school's data system e.g. Sims.Net
5. Adhering to the guidelines of retention of records as defined by School Audit and the Records Management Policy.

5. Responsibilities of Staff

All staff are responsible for:

1. Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
2. 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.
3. If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course 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 Appendix A.

6. Data Security

All staff are responsible for ensuring that:

1. Any personal data that they hold is kept securely.
2. 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.
3. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

4. That the school annually reviews all relevant policies regarding e-safety such as the Information Security Policy and Computer Usage Policy.

7. Personal information should:

1. Be kept in a locked filing cabinet, drawer, or safe; or
2. 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

8. Subject Access Request

All staff, parents and other users are entitled to:

1. Know what information the School holds and processes about them or their child and why.
2. Know how to gain access to it.
3. Know how to keep it up to date.
4. Know what the School is doing to comply with its obligations under the 2018 Act. (See responsibilities of school above)

This Policy document and the School's Data Protection Code of Practise address in particular the last three points above. 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 under the 2018 Act 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 Business manager.
The School will make a charge of up to £10, if a substantial amount of information is requested, to pay for photocopying/postage etc, that access is requested, although the School has discretion to waive this.
The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 working days, as required by the 2018 Act.

9. 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 2018 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 that 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.

10. 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 Long Term Absence Policy or the Equal Opportunities Policy.
Because this information is considered **sensitive** under the 2018 Act, 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.

11. Publication of School Information

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

12. Examples of data

Personal data
Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'personal data' is information which relates to a living, identifiable individual. In the context of this document and the School's requirement to process 'personal data' as part of its duty of care and to educate its pupils, 'personal data' may include:

1. school admission and attendance registers;
2. pupil's curricular records;
3. reports to parents on the achievements of their children;
4. records in connection with pupils entered for prescribed public examinations;
5. staff records, including payroll records;
6. pupil disciplinary records;
7. personal information for teaching purposes;
8. records of contractors and suppliers.

If it is necessary for the School to process certain personal data to fulfil its obligations to pupils and their parents or guardians, then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt (see below), will remain confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

Sensitive data' may include:

9. ethnic or racial origin
10. political opinions
11. religious beliefs
12. other beliefs of a similar nature
13. membership of a trade union
14. physical or mental health or condition
15. offence or alleged offence
16. proceedings or court sentence

Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will be required in writing.

13. Exemptions

Certain data is exempted from the provisions of the Data Protection Act; example include:

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

There are other exemptions under the act

14. 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.

15. Conclusion

Compliance with the 2018 Act 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.

Signed Mr P Mulrooney
Chair of Finance Committee

Signed Mrs V D'Silva
Headteacher
Date _____--

Appendix A

1. Whenever information is obtained from, or received about, individuals, the individuals must know, be told, or have ready access to the following information (or if it is not possible at the point of collecting the information, they must be told as soon as practicable afterwards), regardless of the method of communication used:
· Who they are giving their information to
· Why it is needed and what it may be used for (unless it is obvious from the circumstances)
· Whether it will be used for any other purposes, such as fraud prevention
· Who it may be disclosed to
· How to obtain the information held about them

2. The above information will not have to be supplied if it is necessary to process it solely:

For national security
· For the prevention or detection of crime
· For the apprehension or prosecution of offenders
· To carry out regulatory activities
· As required by law
Or where:
· Information is made public by law e.g. on the electoral role
· Negotiations might be prejudiced
· Legal professional privilege applies

3. Individuals must be told if information is intended to be disclosed outside the school to service providers or external organisations. Schools should be as specific as possible and name organisations or individuals to whom information may be disclosed. Where the list is very long, or there may be different third party service providers in future, then a generic description may be used, such as “healthcare providers” or “other local schools”.

4. If information is required to be disclosed by law, the individuals do not have to be informed of this, but it is good practice to ensure that they are made aware of the statutory requirement to release information about them.
If information is obtained “in confidence” the meaning of this should be explained, if appropriate.

5. It should also be made clear that information may be shared within the school as a whole or with other specific departments.

6. A ‘fair obtaining statement’ can be used as a way of informing individuals of how their personal information will be used when obtaining it. Fair obtaining statements can be used when collecting personal information (e.g. on forms on websites). An example of a fair obtaining statement is outlined below (this can be amended to meet the requirements of different situations):

"Information held by Keresforth Primary School complies with and is stored in accordance with the Data Protection Act 2018. The information you have provided here will be held on the school's information management system and may be disclosed to payroll services and to the DfE for the purpose of monitoring schools."

Related policies:

AUP Policy Staff

AUP Policy KS1

AUP Policy KS2

Confidentiality Policy

Data Breach Procedure

FOI Policy

GDPR

Information Sharing Policy

Information Asset Policy

Information Security Policy

Information Governance Policy

Photographic and CCTV Policy

Records Management Policy

Website Privacy Policy

Privacy Notice – Staff

Privacy Notice – Children

Privacy Notice – Governor

Privacy Notice - LAC