Data Protection Policy

Reviewed Autumn 2016

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

Introduction

Eastway 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, Eastway Primary School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). 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.

Eastway 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, school has developed this Data Protection Policy.

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 school from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controller will deal with day to day matters.

The School's Designated Data Controller is the Headteacher.

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 Headteacher.

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 school of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. School cannot be held responsible for any errors unless the staff member has informed school of such changes.

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 the Data Protection Code of Practice.

Data Security

'Personal data means data which relates to a living individual who can be identified from the data, or from the data and other information which is in the possession of, or is likely to come into the possession of, and includes any expression of opinion about the individual and any indication of the intentions of any other person in respect of the individual.

'Sensitive' data means personal data consisting of information as to the racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), physical or mental health or condition, sexual life, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

All staff are responsible for ensuring that:

• Any personal or sensitive data that they hold is kept securely.

• Personal or sensitive 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.

• Ensure data is subject to a robust password and lock your pc when you are away from the screen to prevent unauthorised use.

• A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information.

Personal or sensitive 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 kept in a locked filing cabinet, drawer, or safe.

All school email is disclosable under Data Protection and FOI legislation. Be aware that anything you write in an email could potentially made public. Agreements entered into by email do form a contract.

Off Site Data
All photographs should be saved to the staff storage drive on our network. No images should be taken off site.

No personal or sensitive data should be stored on memory sticks. All documents containing personal or sensitive data should be saved on the staff area of the network or in a 'cloud based' password protected account such as the school's Google Drive or eschools files.

Rights to Access Information
All staff, parents and other users are entitled to:
• Know what information 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 school is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Data Protection Code of Practice address in particular the last three points above. To address the first point, 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 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 1998 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 make their request in writing and submit it to the Headteacher.

School will make a charge of £10 on each occasion that access is requested, although the Headteacher has discretion to waive this.

School will aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent
In many cases, 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 school processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. 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. 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. This information will only be used in the protection of the health and safety of the individual, but consent is needed to process this data in the event of a medical emergency, for example.

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 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 1998 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.

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.

Retention of Data
School has a duty to retain some staff and student personal data for a period of time following their departure from 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.

Conclusion
Compliance with the 1998 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.

Eastway Primary School Data Protection Policy
Staff and Governor Agreement

I agree to abide by the rules contained in the Data Protection Policy and will follow the principles at all times.

Name: …….. (Please print)

Signed: ……

Date: ……