EASTCROFT PARK PRIMARY SCHOOL

DATA PROTECTION POLICY

Review frequency: At least every 2 years

Approval: Governing body free to determine how to implement.

DFE
Statutory policies for schools
Advice on the policies and documents that governing bodies and proprietors of schools are required to have by law September 2014

Data Protection Policy

1. Introduction

1.1 The Data Protection Act 1998 (DPA 1998) establishes a framework of rights and duties which makes personal information safe. Personal information is information about a living individual, who can be identified from the information. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes, against the right of individuals to respect for the privacy of their personal details.

1.2 Eastcroft Park School is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the DPA 1998. The school has established the following policy to support this commitment. It is the personal responsibility of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this policy.

1.3 Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the DPA 1998. All incidents will be investigated and action may be taken under the school's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and or criminal action being taken.

1.4 This policy explains what our expectations are when processing personal information. This policy should be read together with the policies relating to information security and data retention.

2. Data protection principles

2.1 The DPA 1998 is supported by a set of principles, which must be adhered to whenever personal information is processed. Processing includes obtaining,
2.2 The data protection principles state that personal information must be:

- processed fairly and lawfully;
- processed for specified and lawful purposes;

- adequate, relevant and not excessive;
- accurate, and where necessary kept up to date;
- not kept longer than is necessary;
- processed in line with the rights of the information subject;
- kept secure; and
- transferred only to countries with adequate security.

3. Access and use of personal information

3.1 Access and use of personal information held by the school, is only permitted by employees (temporary or permanent), governors/advisory board members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use for any other purpose is not allowed. Deliberate unauthorised access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

4. Collecting personal information

4.1 When personal information is collected, for example on a questionnaire, survey or a form, the 'data subject' (that is the person who the information is about) must be told, unless it is obvious to them:

- which organisation(s) they are giving their information to;
- what their information will be used for;
- who it may be shared with; and
- anything else that might be relevant, for example the consequences of that use.

This is known as a Privacy Notice.

4.2 Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

4.3 If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose, without the data subject's consent unless there is another lawful basis for using the information (see section 5 below). It

must be made clear to the 'data subject' at the time the information is collected, what other purposes their information may be used for.

5. Lawful basis for processing

5.1 When the school processes personal information, it must have a lawful basis for doing so. The DPA 1998 provides a list of 'conditions' when we can process personal or 'sensitive' personal information. This is contained within Schedule 2 and Schedule 3 of the Act.

5.2 The DPA 1998 defines sensitive personal information as information relating to:

- a person's racial or ethnic origin; political opinion;
- religious or other beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life; and
- criminal offences (alleged or committed).

5.3 Whenever the school processes personal information, it must be able to satisfy at least one of the conditions in Schedule 2 of the DPA 1998 and when it processes 'sensitive' personal information; it must be able to satisfy at least one of the conditions in Schedule 3 of the DPA 1998 as well.

5.4 The school can process personal information if it:

- is necessary to comply with a legal obligation;
- is necessary to protect someone's life or to protect them from serious
- harm;
- is in the public interest and is necessary for the council or another
- organisation to carry out its official duties;
- is necessary for a legitimate and lawful purpose and does not cause
- unwarranted prejudice to the 'data subject'; and
- is necessary to assist in the prevention or detection of an unlawful act.

5.5 The school can also process personal information if it has the data subject's consent (this needs to be 'explicit' when it processes sensitive personal information). In order for consent to be valid it must be 'fully informed' which

means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress.

6. Disclosing personal information

6.1 Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.
6.2 If personal information is given to another organisation or person outside of the school, the disclosing person must identify their lawful basis for the disclosure (see section 4 above) and record their decision. This should include;

- a description of the information given;
- the name of the person and organisation the information was given to; the date;
- the reason for the information being given; and
- the lawful basis.

6.3 If an information sharing agreement or protocol exists, this should be adhered to.

6.4 In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

6.5 When personal information is given internally or externally, it must be given in a secure manner.

7. Accuracy and relevance

7.1 It is the responsibility of those who receive personal information to make sure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded. 'Data subjects' have a right to access personal information held about them and have errors

corrected. More information about a 'data subject's' rights can be found in Section 9 below.

8. Retention and disposal of information

8.1 The DPA 1998 requires the school to not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.

8.2 The relevant guidelines on document retention and destruction must be checked before records are disposed of, to make sure that the prescribed retention period for that type of record is complied with.

9. Individual's rights

9.1 Individuals have several rights under the DPA 1998. These include:

- the right to access personal information held about them (this is known
- as Subject Access);
- the right to prevent their information being used in a way which is likelyto cause damage or distress;
- the right to compensation for any damages as a result of their
- information not being handled in accordance with the DPA 1998; and
- the right to have inaccurate or misleading information held about them
- corrected or destroyed.

9.2 The school has 40 calendar days in which to respond to a Subject Access request, provided the applicant has put their request in writing and suitable identification has been supplied.

10. Reporting security incidents

10.1 The school has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and

monitored. It is only by adopting this approach that the school can learn from its mistakes and prevent losses re-occurring.

10.2 Specific procedures have been developed for the reporting of all information security incidents and weaknesses. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken. Any breaches should be reported to the individual's line manager as soon as the individual becomes aware of the breach. Line managers should report breaches to the Headteacher immediately.

10.3 All employees (permanent, temporary and external users) must be aware of the procedures and obligations in place for reporting incidents and weaknesses which may have an impact on the security of the school's information assets.