Kepier
Believe in you

Policy Statement
Data Protection

- Produced By: Mrs S Prest
  October 2015
- Ratified By: F&GPC
- Review Date: October 2017

DATA PROTECTION POLICY

The Governing Body of the Academy has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Principal and Governors of this Academy intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data are aware of their responsibilities and duties within these guidelines.

Enquiries

All Data enquiries should be made by contacting Kepier, main office on tel. 0191 5128960 email:info@kepier.com

Kepier undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access.

> **"processing"** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
>
> **"data subject"** means an individual who is the subject of personal data or the person to whom the information relates.
>
> **"personal data"** means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
>
> **"parent"** has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

Data Integrity

The Academy undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the Academy of a change of circumstances their computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the Academy will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred

to the Governing Body. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered and all obsolete data will be correctly erased.

Subject Access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a learner, the Academy's policy is that:

- Requests from learners will be processed as any subject access request as outlined below and the copy will be given directly to the learner, unless it is clear that the learner does not understand the nature of the request.
- Requests from learners who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents/carers in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the information/response will be sent in a sealed envelope to the requesting parent/carer.

Processing Subject Access Requests

Requests for access must be made in writing to The Principal.

Learners, parents or staff may ask for access to data. Provided that there is sufficient information to process the request, the request will be recorded, showing the date of receipt, the data subject's name, the name and address of person enquiring (if different), the type of data required (for example Learner Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date).

Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent/carer regarding their own child's record, access to the record will be provided within 15 Academy days in accordance with the current Education (Pupil Information) Regulations.

Authorised Disclosures

The Academy will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Academy may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Learner data disclosed to authorised recipients related to education and administration necessary for the Academy to perform its statutory duties and obligations.
- Learner data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Learner data disclosed to parents/carers in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the Academy.
- Staff data disclosed to relevant authorities for example in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system.
- Only authorised and trained staff will be allowed to make external disclosures of personal data. Data used within the Academy by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the Academy who **need to know** the information in order to do their work.
- A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the Academy.
- An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the Academy's registered disclosures.

Data and Computer Security

Kepier undertakes to ensure security of personal data by the following general methods:

Physical Security

Appropriate building security measures are in place. Only authorised persons are allowed in the computer rooms. Disks, tapes, memory sticks and printouts are locked away securely when not in use. Visitors to Kepier are required to sign in and out, present photo identification and to wear identification badges whilst in the Academy and are, where appropriate, accompanied.

Computer Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement and agree access compliance. All staff have been made aware and trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal or disposed of through confidential disposal services.

Overall security policy for data is determined by the Governors and the Principal, and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Individual members of staff can be personally liable in law under the terms of the Data Protection Act. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.