Data Protection Policy

Category:	Data Protection
Authorised By:	Board of Directors
Signature:	
Signed By:	Barry Nolan
Author:	Sudhi Pathak
Version:	1
Status:	
Issue Date:	April 2016
Next Review Date:	April 2017

Contents

Section	Page
1. Introduction	3
2. Data Controller and the Designated Data Controllers	4
3. Responsibilities of Staff	4
4. Data Security	5
5. Right to Access Information	5
6. Retention of Data	6
7. Monitoring and Evaluation	6

The Eden Academy is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

1. Introduction

1.1 The Eden Academy needs to keep certain information about our employees, pupils and other users to allow us, for example, to monitor performance, achievement, and health and safety.

1.2 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, we must comply with the Data Protection Principles which are set out in the Data Protection Act 1998.

In summary these principles state that personal data shall:

a. Be obtained and processed fairly and lawfully.
b. Be obtained for a specified and lawful purpose
c. Not be processed in any manner incompatible with that purpose.
d. Be adequate, relevant and not excessive for that purpose.
e. Be accurate and kept up to date.
f. Not be kept for longer than is necessary for that purpose.
g. Be processed in accordance with the data subject's rights.
h. Be kept safe from unauthorised access, accidental loss or destruction.

1.3 All staff 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. 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.

2. The Data Controller and the Designated Data Controllers

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

2.2 The School has identified its Designated Data Controllers as:

a. The School Heads
b. The Director of Finance and Operations
c. Office Managers

2.3 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 School Head in the first instance, or with the Director of Finance and Resources if an Academy member of staff.

3. Responsibilities of Staff

All staff are responsible for:

3.1 Checking that any information that they provide to the School in connection with their employment is accurate and up to date.

3.2 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.

3.3 Handling all personal data (eg – pupil attainment data) with reference to this policy.

4. Data Security

4.1 All staff are responsible for ensuring that:

a. Any personal data that they hold is kept securely.
b. 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.

4.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

4.3 Personal information should:

a. Be kept in a filing cabinet, drawer, or safe in a secure office, or;
b. If it is computerised, be password protected both on a local hard-drive and on a network drive that is regularly backed up; and
c. If a copy is kept on a USB memory key or other removable storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer, or safe.

5. Rights to Access Information

5.1 All staff, parents and other users are entitled to:

a. Know what information the School holds and processes about them or their child and why.
b. Know how to gain access to it.
c. Know how to keep it up to date.
d. Know what the School is doing to comply with its obligations under the 1998 Act.

5.2 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.

5.3 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 a request in writing and

submit it to the Head. The School will ask to see evidence of your identity, such as your passport or driving license, before disclosure of information.

5.4 The School may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.

5.5 The School aims 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.

6. 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. Different categories of data will be retained for different periods of time.

7. Monitoring and Evaluation

This is ongoing; where any clarifications or actions are needed the Policy will be amended at its next review.