Data Protection Policy

Diamond Academy

Policy reviewed by Academy Transformation Trust on	Nov 2013
Policy adopted by Local Governing Body on	17 Nov 2014

REVIEW DATE: November 2016

Diamond Academy

Information relating to the Data Protection Policy

The Data Controller is: Diamond Academy

The Data Protection Officer is: Insert name

The Trust/academy will:

- Ensure that there is always one person with the overall responsibility for Data Protection.
- Provide awareness for all members of staff who handle personal information.
- Provide clear lines of report and supervision for compliance with Data Protection.
- Carry out regular checks to monitor and assess new processing of personal data and to ensure The Trust/academy's notification to the Information Commissioner is updated to take account of any changes in processing of personal data.

Content

1 Introduction 4
2 Data shall be processed fairly and lawfully 4
3 Data shall be obtained/processed for specific lawful purposes 4
4 Data held must be adequate, relevant and not excessive 4
5 Data must be accurate and kept up to date 4
6 Data shall not be kept for longer than necessary 5
7 Data shall be processed in accordance with the rights of the data subjects 5
8 Data must be kept secure 5
9 Data shall not be transferred outside of The Trust unless there is adequate protection 6

1 Introduction

1.1 Academy Transformation Trust and our academies need to collect personal information about people we deal with, in order to carry out its business and provide its services. Such people include stakeholders, employees (past and prospective), suppliers and other business contacts.

1.2 In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 1998.

1.3 The lawful and proper treatment of personal information held by The Trust/academy is extremely important to the success of our organisation and in order to maintain the confidence of our employees and stakeholders, we must ensure that we treat personal information lawfully and correctly.

1.4 We support fully and comply with the eight principles of the Act which are summarised in points 2 -9.

2 Data shall be processed fairly and lawfully

2.1 Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

3 Data shall be obtained/processed for specific lawful purposes

3.1 Data obtained for specified purposes must only be used for those purposes identified.

4 Data held must be adequate, relevant and not excessive

4.1 Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

5 Data must be accurate and kept up to date

5.1 Data, which is kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. It is the responsibility of individuals to ensure that data held by The Trust/academy is accurate and up-to-date. Individuals should notify The Trust/academy of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of The Trust/academy to ensure any notification regarding change of circumstances is noted and acted upon.

6 Data shall not be kept for longer than necessary

6.1 The Trust/academy discourages the retention of personal data for longer than it is required. Considerable amounts of data are collected on current staff and pupils. However, once a member of staff or pupil has left The Trust/ academy it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

6.2 In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc. will be retained for the statutory time period (between 3 and 6 years).

6.3 Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 6 months from the interview date. Personnel may keep a record of names of individuals that have applied for, short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

6.4 Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

7 Data shall be processed in accordance with the rights of the data subjects

7.1 Data Subjects have the following rights regarding data processing, and the data that is recorded about them:

- A right of access to a copy of the information comprised in their personal data
- A right to object to processing that is likely to cause or is causing damage or distress
- A right to prevent processing for direct marketing
- A right to object to decisions being taken by automated means
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- A right to claim compensation for damages caused by a breach of the Act.

8 Data must be kept secure

8.1 All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorised third party.

8.2 All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access

- In a locked drawer or filing cabinet
- If electronic, password protected
- Kept on disks which are themselves kept securely.

8.3 Care should be taken to ensure that electronic device screens are not visible except to authorised staff and that passwords are kept confidential. Electronic devices should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

8.4 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant electronic devices should be wiped clean before disposal.

8.5 This policy also applies to staff who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations.

9 Data shall not be transferred outside of The Trust unless there is adequate protection

9.1 Data must not be transferred outside of the European Economic Area (EEA) -the 15 EU Member States together with Iceland, Liechtenstein and Norway -without the explicit consent of the individual. Members of The Trust/academy should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere around the globe. This is because transfer includes placing data on a web site (or file sharing site) that can be accessed from outside the EEA. When sensitive data is passed electronically (such as email) between The Trust/academy and a third party it shall always be in a secure (encrypted) manner.

9.2 All employees will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information
- Understand fully the purposes for which The Trust/academy uses personal information
- Collect and process appropriate information, and only in accordance with the purpose for which it is to be used by The Trust/academy to meet business needs or legal requirements
- Ensure the information is destroyed (in accordance with the provision of the Acts) when it is no longer required
- On receipt of a request from an individual for information held about them by or on behalf of The Trust/academy, they immediately notify Data Protection Officer (DPO)
- Not send any personal information outside of the United Kingdom without the authority of their manager
- Ensure the information is correctly input into the systems.