

Redstone Educational Academy

Data Protection Policy

Rationale

In the course of its work the School needs to access a great deal of data about the students and staff, including personal data and sensitive data. This data needs to be held and used in a responsible manner and the School needs to feel assured that this is and will continue to be the case. Accordingly this policy provides guidance on how the School will hold and use data and seeks to provide the assurances that are necessary.

Guidelines

1. The School will comply with:
 - 1.1 the terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
 - 1.2 information and guidance of which it is aware that is displayed on the information Commissioner's website (www.dataprotection.gov.uk).
2. This policy should be used with the School's **Internet Use Policy**.
3. **Data Gathering**

All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, is covered by the Act.
4. **Data Storage**
 - 4.1 Personal data will be stored in a secure and safe manner.
 - 4.2 Electronic data will be protected by standard password and firewall systems operated by the School.

- 4.3 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
- 4.4 Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.
- 4.5 Particular attention will be paid to the need for security of sensitive personal data.

5. **Data Checking**

- 5.1 The School will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.
- 5.2 Any errors discovered will be rectified as quickly as possible.

6. **Data Disclosures**

- 6.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.
- 6.2 When requests to disclose personal data are received by telephone it is the responsibility of the School to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.
- 6.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the School to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity will be requested.
- 6.4 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- 6.5 Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies the School of a specific legitimate need to have access to specific personal data or if permission has been given by a parent.
- 6.6 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

7 Subject Access Requests

- 7.1 If the School receives a written request from a data subject to see any or all personal data that the School holds about them this should be treated as a Subject Access Request and the School will respond within 20 working days.
- 7.2 Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the School will comply with its duty to respond within 20 working days.

Policy updated: September 2016
Review Date: September 2017

