Washwood Heath
Multi Academy Trust

Data Protection

Policy

1. Data Protection Act

The trust will comply with:

a. 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.
b. Birmingham Education Service and guidance supplied in the Data Protection Advice for Schools flyer and Data Protection Guidance for Schools booklet.
c. Information and guidance displayed on the information Commissioner's website (www.dataprotection.gov.uk).

2. Data Gathering

a. All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
b. Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

3. Data Storage and Disposal

a. Personal data will be stored in a secure and safe manner.
b. Electronic data will be protected by standard password and firewall systems operated by the trust.
c. Computer workstations in administration areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
d. Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
e. Particular attention will be paid to the need for security of sensitive personal data
f. Data is disposed of in accordance with the recommendations contained in 'Records Management Toolkit for Schools (Version 4 – May 2012)', produced by the Information and Records Management Society.

4. Data Checking

a. The academies will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate. Each such request would be logged.
b. Any errors discovered would be rectified and, if incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

5. Data Disclosures

a. 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.
b. When requests to disclose personal data are received by telephone it is the responsibility of the academy to ensure the caller is entitled to receive the data and that they are who they say they are. The request then should be made by fax.
c. 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. Proof of identity should be requested.
d. Personal data will not be used in newsletters; websites or other media without the consent of the data subject.
e. Routine consent issues will be incorporated into the academy's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.
f. Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form, which notifies of a specific, legitimate need to have access to specific personal data. This form is the agreed procedure between Birmingham City Council and West Midlands Police.

6. Subject Access Requests

a. If the academy receives a written request from a data subject to see any or all personal data that the academy holds about them, this should be treated as a Subject Access Request and the academy will respond with the 40 day deadline.
b. Informal requests to view or have copies or 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 academy will comply with its duty to respond within the 40 day time limit.

7. CCTV

CCTV is also treated securely.

8. School Issued Laptops used off-site

Members of Staff are issued laptops to facilitate their job role. These laptops are encrypted by the IT technicians before issue and staff members are given an encryption password that they are able to change. Any portable data device with personal and sensitive information on must be encrypted also.

9. Data Protection Incidents

All colleagues receive annual data protection training in which they are told to report data protection incidents, concerns or ask for advice when required directly to the Senior Information Risk Officer (SIRO), within each Academy in first instance, or the Executive Head Teacher in their absence/unavailability. A disclosure log is maintained of all data protection breaches.