

COTTESBROOKE INFANT & NURSERY SCHOOL



Data Protection Policy

- 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 Birmingham City Council's advice and guidance.
 - 1.3 Information and guidance displayed on the Information Commissioner's website.

- 2 This policy should be used in conjunction with the school's ***Internet Usage Policy***.

- 3 Data Gathering
 - 3.1 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.
 - 3.2 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.

- 4 Data Storage
 - 4.1 Personal data will be stored in a secure and safe manner. Any physical loss of data must be reported to the Head Teacher in his capacity of SIRO.
 - 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 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.
 - 4.6 Identifiable data will only be stored on school issued encrypted data devices.

- 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 would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

- 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 should be requested.
 - 6.4 Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought at Christmas, should include the names of any children where parents have consented to its use and only display forenames and the first initial of the surname.
 - 6.5 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
 - 6.6 Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.
 - 6.7 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.
 - 6.8 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 which the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.
 - 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 the 40 day time limit.
- 8 Data Destruction
- 8.1 Documents are retained in accordance with their legal requirements. Electronic data is destroyed professionally by an external agency; paper documents are shredded on site.
- 9 This policy will be included in the *Staff Handbook*.
- 10 Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.