YORKMEAD JUNIOR INFANT SCHOOL

DATA PROTECTION POLICY

Yorkmead School is committed to safeguarding and promoting the well-being of all children, and expects our staff and volunteers to share this commitment.

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 Education service advice and guidance supplied in the Data Protection Advice for Schools flyer and Data Protection Guidance for Schools booklet.
   - 1.3 Information and guidance displayed on the information Commissioner's website (www.dataprotection.gov.uk)

2. This policy should be used in conjunction with the school's Internet Use 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.
   - 4.2 Electronic data will be protected by an encrypted 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 Physical data will be stored where it is not accessible to anyone who does not have 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 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 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 politely be refused as permission would be needed from all the data subjects contained in the list. (Note: a suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem).

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. These will be made at the beginning of every academic year.

6.7 Personal data will only be disclosed to Police Officers if they are unable 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 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 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. Advice will also be sought from Birmingham City Council.

8. This policy will be included in the Staff Handbook.

9. Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.

Appendices

- Pupil data gathering sheets/covering letter
- Pupil data checking sheet/covering letter
- Staff data gathering sheets/covering letter
- Reception initial enquiry data gathering sheet
- School transfer initial enquiry data gathering sheet

This Policy will be reviewed in March 2018 .

Signed_____ Chair of Governors

BIRMINGHAM CITY COUNCIL

POLICY STATEMENT ON DATA PROTECTION

1 Scope

This policy applies to all personal data held by the City Council. It encompasses paper records; data held on computer and associated equipment, including CCTV, of whatever type and at whatever location, used by or on behalf of the City Council.

The obligations outlined in this policy statement apply to all those who have access to personal data, whether employees of associated organisations or volunteers. It includes those who work at home or from home, who must follow the same procedures as they would in an office environment.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to prosecution. All individuals permitted to access personal data must agree to comply with this policy.

2 Confidentiality and Security

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in the Data Protection Act 1998.

- Paper records will be managed so that access is restricted to those who need to use the information and stored in secure locations to prevent unauthorised access.
- Computer systems will be designed and computer files created with adequate security levels to preserve confidentiality. Those who use the City Council's computer equipment will have access only to the data that is both necessary for the work they are doing and held for carrying out that work.
- Personal data will be disclosed only to the data subject and other organisations and persons who are pre-defined as notified recipients.

Data users must comply with specified security measures; which are detailed in the City Council Information Security Policy and Information Security Guidelines and Checklists documents.

3 Ownership of Data

Each City Council department is responsible for the personal data that it holds. This responsibility extends to data that is processed by a third party. The department will hold a record of all data files that is owns containing personal data, whether on paper or electronic media. Where required, the department will provide necessary information on IT Customer Services to facilitate the notification of the data with the Data Protection Commissioner.

4 Collection of Data

The City Council will inform data subjects of the reason why the data is being collected and to whom the data may be disclosed.

5 Contents of Accuracy of Data Files

The City Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort must be made to ensure that the data is accurate and up-to-date and that any inaccuracies, once discovered, are corrected immediately.

6 Processing

All processing of personal data will comply with the Data Protection Principles as defined in the Data Protection Act 1998. In the situation where data is processed by a third party, the third party will be required to act in a manner which ensures compliance with the Data Protection Act 1998.

Data will only be processed for the purpose which it was collected and should not be used for additional purposes without the consent of the data subject.

7 Disclosure of Information

Personal data must not be disclosed, except to users authorised to receive that data, other organisations and people who are pre-defined as notified recipient, without the permission of the data subject.

In cases where the Council performs the functions of a computer bureau for a third party, no disclosure of information will be made without the permission of the third party concerned.

8 Access to Personal Data

The City Council will provide on request of any individual information regarding their personal data with a statement of whether or not the City Council holds personal data about them. If it does hold personal data, then it will provide a written copy of the current data held about them and details of disclosures that have been made. (The information will not include associated information relating to another individual who has not given permission for a disclosure to be made). The information will be provided as soon as possible within a period prescribed by the Data Protection Act.

The Data Protection Registrar states that a fee per request can be charged and the City Council may do this at its discretion.

Data may be withheld in specific circumstances defined in the Act or within other legislation. The Council may also refuse to meet requests for information which the appropriate Chief Officer believes to be made with undue frequency. In deciding on the nature of "undue frequency", regard will be had to the sensitivity of the information held and the frequency with which it is changed or updated.

To minimise the risk of accidental misidentification or deliberate impersonation, the appropriate officer must ask applicants to supply sufficient information to enable them to be satisfied about the identities of persons making requests.

9 Correction of Inaccurate Data

When, as the result of an enquiry, a material inaccuracy or omission is discovered, the personal data must be corrected or erased immediately. If the data has been disclosed to a third party, then the third party must be informed of any corrections.

10 Training

All council personnel that work with personal data, and their managers, must receive training in the area of Data Protection.

This policy will be reviewed in **July 2018**.

Signed: _____ Chair of Governors

Dated: _____