# GREEN MEADOW PRIMARY SCHOOL

# Data Protection Policy

Reviewed by Governors : 24th March 2017

To be reviewed next : March 2018

An Academy, achieving more, learning together.

**Green Meadow Primary 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 Children, Young People and Families Directorate 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.

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.

**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 be politely

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.

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 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 school will comply with its duty to respond within the 40 day time limit.

8 This policy will sit alongside 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.

**10 Home Working**

School staff may wish to undertake work at home and this will often involve the use of ICT equipment that will hold databases containing personal data. Similarly, paper files containing personal data may also be used away from the school environment.

Permission should always be obtained before processing personal data at home and it should be remembered that the definition of "processing" includes "holding" even if the information is not actually used (i.e. a file is taken home that normally wouldn't be used in everyday nature of job)

Staff should always take reasonable measures to ensure no unauthorised access can be made to the personal data taken home. This is likely to mean that computers are password protected and are not left unattended with personal data accessible. Staff should take special care in ensuring that paper files are kept secure and locked away when not in use. This will ensure that individuals, including family members, do not have access to the personal information, thus ensuring protection against potential unauthorised disclosure, accidental loss or destruction.

Employees who choose to undertake work at home in relation to their official duties using their own ICT equipment must understand that they are not permitted to hold any database, or carry out any processing, of personal data relating to the school.

Extra care should be taken when transporting personal school data out of school. Personal files should be transported in a secure manner. For example personal files should not be left in clear view in unattended vehicles or outside vehicles without the responsible member of staff being present.

## 11 Day to Day Working

The following points are intended to act as a guide for staff to follow when using personal information during the working day:

11.1 Unauthorised staff and other individuals should be prevented from gaining access to personal information.

11.2 Visitors should be received and supervised at all times within the school premises, especially where information about individuals is stored.

11.3 All computer systems containing personal data should be password protected; the level of security will depend on the classification of data being held. Staff must lock their computers if walking away.

11.4 Staff should have access to personal information on a "need to know" basis.

11.5 Computer workstations should not be left signed on when not being used.

11.6 CDs, disks, tapes, printouts and other storage media containing personal data should be locked away when they are not in use.

11.7 Be careful about what is sent via email and to whom information is sent. Check with the recipient before sending personal data that email will be an appropriate way for them to receive that data.

11.8 Check that the intended recipient of a fax containing personal information is aware that it is being sent in order that they can ensure security on delivery.

11.9 Ensure that paper files are stored in secure locations and accessed on a "need to know" basis only.

11.10 Do not disclose personal information to anyone other than the data subject unless you have his or her consent, it is a registered disclosure, or it is required by law or permitted by a Data Protection Exemption. **Always ask for proof of identity before making a disclosure – see below for further information.**

11.11 When processing personal information do not leave it on public display. All paper files containing personal information should be locked away at the end of each day and not left on desks.

11.12 Computer monitors should be positioned so that personal data cannot be viewed by anyone not authorised to do so.

11.13 Security arrangements should form part of a written agreement between the data controller and data processor, if processing is carried out by an external source.

11.14 Subject to relevant retention periods, redundant personal data will be destroyed by shredding.

- CDs, disks, tapes, and other storage media are physically destroyed beyond recovery. Computers being sent away for repair must be checked by the user to ensure databases have been removed.
- Computers are destroyed at an approved secure disposal recycling site.
- Staff are requested to store more 'sensitive' data (eg SEN) on the schools network drive. This drive is only available in school and therefore would not be visible if a laptop was stolen/lost.

11.15 CCTV images are recorded for safety and security purposes. Recordings will be retained for 2 weeks and only copied for longer storage in the event of an

investigation. After such investigation has concluded, the copied recording will be securely deleted.

## 12 Disclosing Information to the Data Subject (i.e. a child, mom or dad)

Before disclosing any personal information you must be satisfied that you are talking to the data subject by asking for proof of identity. If they have no proof of identity or the enquiry is over the telephone, the following procedure should be followed:

12.1 Ask two questions, which you believe only the data subject could answer, i.e. reference number, payment details, family names etc.

12.2 The data subject must answer at least two questions correctly before you disclose any personal information to them. If you are at all unsure of the individual's identity or your questions were not answered correctly ask more questions.

12.3 If you are still unsure of the data subject's identity, apologise to the person/caller and explain that you cannot give out any personal information because under the terms of the 1998 Data Protection Act you are unsure of their identity. Advise them to write or return with suitable identification if the information is still required.

12.4 If you are satisfied that you are speaking to the data subject and they have answered at least two questions correctly, they can only be supplied with information which relates to themselves in order to deal with their enquiry.

## 13 Disclosing Information with the Data Subject's Consent

If an organisation or individual calls and requests information about an individual, the data subject's consent must be gained before any information is disclosed, unless there is a legal reason for the disclosure. Such consent may have been given at the point of collection of the personal data, if the person or organisation was listed as a possible disclosure to which the data subject agreed by completing the form.

Should the request be by telephone, first check the caller's identity. To do this check the telephone number by calling them back.

If you are at all unsure of the caller's identity you can refuse to disclose information over the telephone and ask the caller to put their request in writing.

When such a disclosure is made, there must be an entry made in the disclosure log held in the office.

## 14 Freedom of Information.

The data subject has the right to see all of their personal information (unless covered by an exemption). However, there are clear protocols that must be followed. We reserve the right to levy a fee to cover administration costs of £10.00.

For further information on this area please see the Freedom of Information Policy.

## 15 Photographs

Photographs can be taken by parents for personal use (eg. sports day, trips, assemblies).

The Data Protection Act only limits photography if the images will be used for an official purpose (eg. Website etc.)