Deanery C.E. Primary School

Data Protection Policy

DATA PROTECTION POLICY

1. Purpose

Deanery C.E. Primary School is committed to protecting and respecting the confidentiality of personal and sensitive information relating to staff, pupils, parents and governors held on file or electronically. The purpose of this policy is to ensure compliance of Deanery C.E. Primary School and all of its' stakeholders with the obligations set out in the eight Data Protection Principles contained within the Data Protection Act 1998. This policy applies to all staff, parents, governors and visitors of the School.

2. Data Controller

The School, as a body, is the Data Controller under the 1998 Data Protection Act, and the Governors are therefore ultimately responsible for implementation. However, the school has identified its Designated Data Controller as the Headteacher. Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Head Teacher in the first instance.

3. Definitions

Data is information that relates to an identifiable living individual that is processed as data:
• is processed automatically;
• is recorded with the intention that it should be processed automatically;
• is structured as part of a relevant filing system in such a way that information relating to an individual is readily accessible;
• forms part of an accessible record.
Personal data is data held electronically or in structured files that tells you something about an identifiable living individual. Examples would be names, dates of birth, school marks, exam results, SEN and medical information, performance reviews, addresses and telephone numbers which are especially vulnerable to abuse, but so are names and photographs if published in the wider environment of the press, Internet or media.
Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data.
Processing covers everything from obtaining to destruction. For example, collecting, recording, using, operating, disclosing, storing information or disposing of data.
Data subject is the person to whom the information relates. In the case of most children, who are unable to understand the principles of data protection, the data protection interests will be represented by the parent or guardian.
A **data processor** is any person (other than an employee of the data controller) who processes data on behalf of the data controller.
A **recipient** is any person to whom data is disclosed.
An **authorised disclosure** of information is one for which permission has been received from the data subject.
An **unauthorised disclosure** of information is one for which permission has not been received from the data subject. Unauthorised disclosure may lead to prosecution of either or both the person and organisation responsible.

4. Data protection principles

First Principle - Fair and Lawful Processing

"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 of the Data Protection Act is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act is also met".

These are some examples of the current uses of data and the implications for use:
- monitoring performance of children; names and ethnic groups are shared between staff on an LEA maintained secure website/database called E-portal and are also shared with Church of England Birmingham, as examined by OFSTED e.g. boys v girls etc.
- paper files of analysis of strengths/weaknesses is also shared between the year group in their assessment folders – these folders are kept in a secure location.
- each year, a 'contacts' sheet is completed and returned to the office by parents, this contains addresses, phone numbers and medical conditions. These are kept in the office on a computer system that all staff can access. There is one paper copy in a file for emergencies, in case of computer failure. These files are kept in a lockable cupboard in the office.
- class lists and contact details are photocopied and taken off site when on trips. Upon return these sheets are shredded.
- medical information is kept on a centralised computer file and is distributed to relevant class teachers and staff at the start of the academic year.
- children with life threatening or serious conditions have information on the inside lid of attendance register boxes. This information is also displayed on the inside of cupboards within the relevant classrooms so that staff are aware. There is also a board in the kitchen so that kitchen staff are aware of allergies. Parents are informed of how this 'serious condition' data is used when the medical sheets are completed.

Second Principle – Specified Purpose

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

The school has to subscribe to the Information Commissioner's Office (ICO) annually and identifies how data is used. The School is responsible for notifying the ICO of any changes to the purpose of processing personal data.

Third Principle - Adequate, Relevant and Not Excessive

"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."

The Deanery will only collect, retain and distribute date that is necessary to complete tasks.

Fourth Principle – Accurate

"Personal data shall be accurate and, where necessary, kept up to date."

Individual pupil data checking sheets will be issued annually to remind parents of the importance of supplying accurate data. Personnel data will be kept up-to-date and reminders will be issued every September by the Business Manager.

Fifth Principle – Not Kept Longer Than Necessary

"Personal data processed for any purposes shall not be kept for longer than is necessary for that purpose or those purposes".

Our Retention Policy specifies our document retention periods. Special Educational Needs information must be kept for 20 years and is stored securely on school premises. All other data (e.g. year 6 leavers) is kept for one year before being securely destroyed (shredded).

Sixth Principle – Data Subjects' Rights

"Personal data shall be processed in accordance with the rights of Data Subjects under this Act".

A person will contravene this principle if they:
• Fail to properly respond to a Subject Access Request
• Fail to respond to notices from individuals exercising their rights:
- to prevent processing likely to cause damage or distress
- to prevent processing for direct marketing
- to prevent processing in relation to automatic decision taking.

Seventh Principle – Security

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

The school maintains high levels of security in order to safeguard the children and all personal data is kept in lockable cupboards. Portable electronic devices must be encrypted and strong passwords must be used to protect data.

Eighth Principle – Overseas Transfer

"Personal data should not transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

5. Staff and Governors responsibilities

The following points are intended to act as a guide for staff and governors to follow when using personal information during the working day. Staff and Governors are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date which includes informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment

or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

- Handling all personal data (e.g. – pupil attainment data) with reference to this policy.
- Ensuring personal information is not disclosed either orally or in writing or via the internet or by any other means, accidentally or otherwise, to any unauthorised third party.
- Ensuring that unauthorised staff and other individuals should be prevented from gaining access to personal information.
- Escorting and supervising visitors at all times within the school premises, especially where information about individuals is stored.
- Protecting all computer systems containing personal data, these should be password protected (see IT Policy). Staff must lock their computers if walking away (i.e. use windows key (flag) and L)
- Staff should have access to personal information on a "need to know" basis.
- Making sure electronic storage devices containing personal data (e.g. memory sticks, ipads, phones) is kept secure and password protected. Electronic storage devices should be locked away when they are not in use.
- Being careful about what is sent via email and to whom information is sent. Personal data sent to an external email should be sent in a password protected document with the password sent in a separate email. Best practice is to use initials rather than pupil names.
- Checking 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.
- Ensuring that paper files are stored in secure locations and accessed on a "need to know" basis only.
- 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 "Right to Access Information" below for further information.**
- 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.
- Staff should not remove personal or sensitive data from the School. 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.
- Extra care should be taken when transporting files to and from home. Laptops or files should be transported in a secure manner and not left on a seat, the roof of the car or on the pavement.
- Subject to relevant retention periods, redundant personal data will be destroyed by shredding for physical files and IT storage media devices should be wiped and physically destroyed beyond recovery. (See also Data Retention Policy)

6. Rights to access information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

The School will, upon request, provide all staff and parents and other relevant users with a fair processing notice (see Appendix 3) regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. The School will ask to see evidence of your identity, such as your passport or driving licence, before disclosure of information.

The School may make a charge £10 on each occasion that access is requested in order to meet the costs of providing the details of the information held.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

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

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

8. Photographs

Photographs can be taken by parents for personal use (e.g. sports day, trips and assemblies) but these must not be shared or published on social media sites. Photographs taken within school will only be used with the permission of parents and these photos will be stored securely and are covered by the Data Protection Act.

9. CCTV

The School operates a CCTV system for security purposes and stores images for 10 days before they are overwritten. On occasion images are copied and stored for longer periods for further investigation (e.g. suspicious activity).

10. Retention of Data

The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time, please refer to our Data Retention Policy.

Policy reviewed by Jayne Luckett *September 2016*

Agreed and accepted by Governing Body *September 2016*

*Signed*_____

Dated _____

Data Protection Policy – Appendix 1

Frequently Asked Questions

Q: **A teacher wants addresses or telephone numbers on a class list - is this okay?**
A: Consider why? If the teacher is taking pupils away on an overnight journey, then the information is necessary. Please, however, remind the teacher that the printout should be kept private and be returned to the school office for shredding immediately after the event. Otherwise, no - if the teacher needs to know such details, they will be available from the school office.

Q: **At Christmas, parents are requesting lists of children in their child's class, to enable them to send cards to all the children and avoid anyone missing out. Is this okay?**
A: A list of just forenames is okay as this information will be freely available to the children in class anyway and is therefore considered to be in the public domain. If you prefer, allow older children who can write time in class to write out their own list.

Q: **The school nurse has noticed a medical condition and wishes to speak to the child's parents about treatment. Can I release the address?**
A: Consider whether the nurse is working in an official capacity for your school? If the answer is "yes" telephone the parent to request permission, once obtained go ahead and record the information in your Disclosure Log. The above item would apply to other people working in an official capacity for your school and could include school dentists, doctors, welfare officers, social workers who you know to be involved with the pupil. Always record the disclosure in your log - you will have forgotten it by the following week!

Q: **A private dentist is setting up in the area and would like to mail-shot our families -can I give him the addresses?**
A: Do you really need to consider it? The answer is "no" – it is not an authorised disclosure. There are circumstances like this where you may consider distribution of mail via the pupils.

Q: **The school photographer wants to print names on to the frame of a group photograph. Is this okay?**
A: Consider whether there any families who would rather not have their children so identified? All parents should give their written permission - this may sound like unnecessary overkill but is not as drastic as it sounds. The problem of pupil recognition by those with a sinister purpose cannot be understated. You really have to consider what control you have over materials where the information is printed.
Consider the possibility of an estranged father - denied all access - recognising his daughter from a photograph and abducting her because he has just discovered which school she now attends.

The next example is a very common one that affects all schools from time to time:
Q: **The local newspaper wants to publish a photograph of a school event. Of course, the children want their names in print - can I release them?**
A: Consider what control you have over the distribution of the newspaper? – the answer to this is absolutely none. You should have permission from the parents of the children in the photograph. If you don't get it, then the text might read:". ...children from the school". Please make sure that neither teachers nor children themselves release their names to the reporter, if parental permission has not been obtained. The above example applies equally to television reports and video productions.

Q: **I want to put pupil names and/or photographs on the Internet. Can I?**
A: Remember that all information passed to the Internet goes beyond your control and can be accessed worldwide, including in countries without adequate data protection legislation. Digital photographs and scanned images where pupils can be identified are also covered by the 1998 Data Protection Act, so get written parental permission to place photographs on the website but never post the name with the photograph!

Q: **The police want information about one of our pupils who has been up to no good. Surely I can release that?**
A: Always ensure that the police provide a WA170 declaration form that is signed by the rank of Inspector above and proves that you have taken reasonable care to ensure police entitlement to the personal data. Also, only give them what is necessary, not whole files or print-outs relating to a pupil.

Q: **A parent wants to see what information we hold about his or her child. What do I do?**
A: The parent should make a formal written Subject Access Request or, if you wish to deal with the situation less formally, agree a mutually convenient place and time to show them their child's records. You must respond to formal requests within the 40-day deadline.

Q: **A parent refuses permission for us to hold the child's information on our computer. What do I do?**
A: Be diplomatic! You have the right to hold the information that you need for administering the child's progress through your school and to disclose it within the terms of your notification and the provisions of the Act.

Q: **A parent wants to take the child to a friend's party. Can I release the address?**
A: No - you should telephone the party-holder and do it that way.

Q: **I think that it's a good idea to put the addresses, telephone numbers and email contact details of our Governors in the School Prospectus. Does that present any problems?**
A: It's a good idea but Governors make decisions that may not be universally popular. Perhaps the release of a telephone number may cause problems. If you particularly want to publish such details, ask the person concerned to sign a note agreeing to the publication of their contact details. If they do not agree, they can still be contacted via the school.

Q: **A teacher has applied for a mortgage and the building society has requested that I confirm the person's post and salary. Can I do this?**
A: Yes, but just ask the person to write a note requesting you to do so.

Data Protection Policy – Appendix 2
Case Studies

Somewhere in the south of England, a police officer in uniform approached a secondary school secretary and asked for the address of a pupil who he named and said he wished to discuss an incident with him. The police officer said he did not wish to speak to the pupil in school as he may be unfairly judged if he was seen to be questioned by the police at school. This seemed reasonable to the secretary who gave the police officer the pupil's address. Unfortunately, the real reason the officer wanted the address was that this boy had supplied his own teenage daughter with drugs. He went round to the boy's house and beat him up, injuring him so severely the boy ended up in hospital. The police officer ended up being dismissed from his job and jailed for the assault but, more importantly from a data protection angle, the school secretary was fined for making an unauthorised disclosure of personal data.

A few years ago the national press quoted the case of a convicted paedophile, subsequently released from prison. From his prison cell he made secret plans to re-offend. He got hold of copies of his local newspaper and scoured them for pictures of young girls. He noted the names of dancers and youngsters in school pictures, preparing for the time when he would once again prowl the streets of his hometown and holiday resorts. Detectives believe he resumed preying on children as soon as he was freed. He used telephone books to find addresses of children he had identified in pictures. He then visited addresses, engaging youngsters in conversation outside their homes. With a methodical attention to detail typical of many paedophiles, he used a map book of the town and the surrounding area, marking the homes of children with their initials. During their inquiry, police spoke to seventy children aged from six to fifteen, who had some link with him.

Deanery C.E. Primary School

Fair Processing Notice

Our policy for handling personal data

Deanery C.E. Primary School handles personal information in compliance with the Data Protection Act 1998 (the Act). We recognise the importance of the correct and lawful processing of personal data in maintaining confidence in our operations. We fully endorse and adhere to the principles set out in the Act.

Deanery C.E. Primary School registration as a data controller

Deanery C.E. Primary School is a 'data controller' under the Act. Deanery C.E. Primary School holds information for the reasons given to the Information Commissioner and may use the information for any of those reasons.

Deanery C.E. Primary School has notified the Information Commissioner that we will process personal data to enable us to provide our actuarial services to our clients, to maintain our own accounts and records and to support and manage our staff. The Information Commissioner describes the processing in a register which is available to the public for inspection at http://www.ico.org.uk/. Deanery C.E. Primary School's entry on this register can be viewed here.

The key reason we process personal data is in relation to the provision of educational services. Deanery C.E. Primary School is committed to protecting and respecting the confidentiality of personal and sensitive information relating to staff, pupils, parents and governors held on file or electronically.

Personal data

This policy applies to the handling of personal data. This is data relating to a living individual who can be identified from the data, or from that data and other information which we hold or which is likely to come into our possession. It includes names and email addresses of subscribers to our publications or personal details held in relation to our work for our clients. It also includes any expression of opinion about an individual or any indication of our intention in respect of them.

Processing information fairly and lawfully

Deanery C.E. Primary School processes information only where:

a) the law allows us to, or

b) you have given your consent, or

c) we have received a court order

Ensuring your personal information is safe and accurate

Deanery C.E. Primary School ensures that information held on our computer systems and in our paper filing systems is secure to guard against unauthorised or unlawful processing or accidental loss, destruction of, or damage to personal data. In order to carry out its functions Deanery C.E. Primary School may receive information about you from others or give information to others, but we can only do this in accordance with the law. Any third parties from whom we receive personal data or to whom we pass personal data are also required to comply with the Data Protection Act.

Deanery C.E. Primary School only collects and records personal information that is necessary to carry out its functions, nothing more. The information that we record is based on fact and, where opinion is recorded, it is relevant and backed up by evidence. To the extent it is

reasonable and appropriate to do so, Deanery C.E. Primary School checks that the personal information being recorded is accurate.

Data sharing
Deanery C.E. Primary School will only share personal data with those organisations that it is legally able to, and where sharing personal data is necessary we will comply with the Data Protection Act.

Retaining information
We will only retain the information if a business need exists. It is not kept longer than is necessary for that purpose. To this end, Deanery C.E. Primary School has in place and applies a formal retention policy for recorded information.

Your rights to access your personal information
Under the Act you have the right to ask to see the information which Deanery C.E. Primary School holds about you and why. If you want to see the information we hold about you then you must ask for the information in writing and give your full name and address. You should send your request to:

The Data Protection Officer
Deanery C.E. Primary School
14 Fox Hollies Road
Sutton Coldfield
B76 2RD
email: enquiries@deanery.bham.sch.uk