Savile Park Primary School

Data Protection Policy

Version	**12/16**
Name of Policy Writer	**EducateHR Ltd**
Date Written	**April 2013**
Last Updated	**December 2016**
Next Review Due	**December 2017**

Contents **Page**

1. Introduction

1.1 In order to operate efficiently the school has to collect and use information about people with whom it works. These include pupils, employees, suppliers, volunteers and others.

1.2 In addition the school is also required by law to collect certain specified information in order to comply with the requirements of central government departments.

1.3 This personal information must be handled and dealt with properly and the school is committed to compliance with the requirements of the Data Protection Act 1998 ("the Act").

1.4 The school will ensure that all employees, trainees, external contractors, volunteers, governors, consultants and partners of the school who have access to any personal data are fully aware of their responsibilities under the Act.

2. Purpose and scope

2.1 In the course of their work many school employees will be required to process personal data in accordance with the Data Protection Act 1998. This policy will help school employees to understand the legislation and their responsibilities to ensure that the Act is not breached.

2.2 All school staff must be aware that breaches of data protection legislation can lead to both criminal and civil liability.

3. The Information Commissioner's Office

3.1 The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

3.2 The ICO maintains a public register of data controllers. Each register entry includes the name and address of the data controller, together with a general description of the processing of personal data carried out.

3.3 Notification is the process by which details of data controllers are added to the register. The Data Protection Act 1998 requires every data controller who is processing personal data to notify unless they are exempt. The school is registered as a data controller.

3.4 Further detailed information regarding the register can be found at http://www.ico.gov.uk/ Contact details for the ICO are:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Enquiry/Information Line: 01625 545745

4. The 8 principles of the Data Protection Act 1998

4.1 The law of data protection seeks to balance the rights of individuals to privacy with the need of the relevant body (in this case the school) to process personal information for legitimate purposes. Legislation applies only to information about living individuals who can be identified from that information.

4.2 The Act requires that eight data protection principles be followed in the handling of personal data. These are that personal data must:

1) be fairly and lawfully processed
2) be processed for limited purposes and not in any manner be incompatible with those purposes
3) be adequate, relevant and not excessive
4) be accurate
5) not be kept for longer than is necessary
6) be processed in accordance with individuals' rights
7) be secure
8) not be transferred to countries without adequate data protection.

5. Definitions

5.1 All of the following definitions relate to the Data Protection Act 1998.

5.2 **Data** means information that is:

- held on computer, or recorded with the intention that it will be put on computer at a later date
- contained in a paper-based filing system, or kept with the intention that it will be added to such a system at a later date
- part of an 'accessible record' – this includes education records.

5.3 The Act will therefore apply to most of the personal information held by the school whether on computer or in paper files.

5.4 **Personal data** is data which relates to a living individual who can either be identified from the data or from any other information which the data controller has or is likely to have. If the subject of the data is dead, then the information held cannot be personal data.

5.5 A **data subject** is a living individual who is the subject of personal data.

5.6 **Processing** means obtaining, recording or holding information or data, or carrying out any operation on the information to organise, adapt, alter, retrieve, consult, use or disclose, ie all activities, including storage.

5.7 The **data controller** is the person, who, either alone or jointly with others, decides upon the purposes for which and the manner in which any data are, or shall be, processed. In the case of the school the data controller is the organisation itself.

5.8 The Act also provides conditions for processing of any personal data and makes a definite distinction between "**personal data**" and "**sensitive personal data**".

5.9 **Personal data** is defined as data relating to a living individual who can be identified from that data such as:

- salary and bank account details held either on a computer or in a manual filing system
- an email about an incident which names a member of staff or a pupil
- a line manager's records which contain sections on named members of staff
- a line manager's notebook containing information on only one individual, but where there is an intention to put that information on file
- a set of completed application forms
- any other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

5.10 **Sensitive personal data** is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexual orientation or practice
- criminal proceedings or convictions.

6. Handling of personal/sensitive information

6.1 The school will, through appropriate management and the use of strict criteria and controls:

- observe fully conditions regarding the fair collection and use of personal information
- meet its legal obligations to specify the purpose for which information is used
- collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of information used
- apply strict checks to determine the length of time information is held
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the rights of people about whom the information is held can be fully exercised under the Act.

6.2 These include certain rights:

- the right to be informed that processing is being undertaken
- the right of access to one's personal information within the statutory 40 days
- the right to prevent processing in certain circumstances
- the right to correct, rectify, block or erase information regarded as wrong information.

6.3 In addition, the school will ensure that:

- an identifiable individual within the school is charged with specific responsibility for data protection (and in this school that designated person is the Information Officer).

6.4 The school will also ensure that:

- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- everyone managing and handling personal information is appropriately trained to do so
- everyone managing and handling personal information is appropriately supervised
- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are regularly assessed and evaluated
- performance with handling personal information is regularly assessed and evaluated
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing
- any disclosure of personal data will be fully in compliance with approved procedures.

6.5 All managers and staff within the school will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- paper files and other records or documents containing personal/sensitive data are kept in a secure environment
- personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically
- individual passwords should be such that they are not easily compromised.

6.6 All contractors, consultants, partners or other servants or agents of the school must:

- ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the school, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act

- be aware that any breach of any provision of the Act will be deemed as being a breach of any contract between the school and that individual, company, partner or firm
- allow data protection audits by the school of data held on its behalf (if requested)
- indemnify the school against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

6.7 All contractors who are users of personal information supplied by the school will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the school.

7. Implementation

7.1 The school has appointed XXX (insert named individual) as an Information Officer with specific responsibility for data protection in the school. The Information Officer will be responsible for ensuring that the Data Protection Policy is implemented.

7.2 The Information Officer will also have overall responsibility for:

- the provision of cascade data protection training, for staff within the school
- the development of best practice guidelines
- the performance of compliance checks to ensure adherence with the Data Protection Act.

8. Subject Access Requests

8.1 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 should respond within the statutory deadline of 40 days.

8.2 The school may charge a fee, up to a maximum of £10, for complying with the request. The 40 day period starts either when the fee is received, or from the date the request arrived in written form, if no fee was asked for.

8.3 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.

9. References

9.1 There is no general exemption in the Data Protection Act 1998 with regard to references. However, there is a special exemption from an individual's right of access to information if the reference is in the hands of the organisation which produced it, ie before it has been sent to the potential employer.

9.2 Once the reference is in the hands of the organisation or the person to whom the reference was given, this exemption no longer applies, ie the member of staff does not have automatic access to a reference written **by the school/academy in which they work**.

9.3 Once the reference has been sent to the person who had requested it, the individual can then request access. In all instances, the person who requested the reference is entitled to withhold any information given within the reference that would identify a third party. This definition of third party includes the person who wrote the reference.

10. Retention periods

10.1 In relation to the retention of records, the school follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code. (These are reproduced in Appendix 2.)

10.2 The periods stated in Appendix 2 should therefore be treated as appropriate guidelines for retention times in the absence of a specific business case supporting a longer period.

11. Other Policies and Procedures

11.1 This policy will be supported by the following policies and procedures:

- Freedom of Information Policy
- School Policy on Use of Internet and Emails
- School Security Procedures

Appendix 1: Subject Access Request Form

Organisation Logo here

Subject Access Request Form

1. *YOUR DETAILS (BLOCK CAPITALS PLEASE)

Surname:	First names:
Title:	Any other names used (e.g. maiden name):
Date of birth:	
Current address: Postcode:	Previous address: Postcode:
Daytime telephone number:	
Email address:	

*****You will be asked to provide proof of your identity and address. Please see the Guidance Notes attached.

2. WHOSE INFORMATION ARE YOU REQUESTING? (Please tick relevant box)

- **My own** ☐
- **Someone else's** ☐
- **Both my own and someone else's** ☐

3. *IF YOU ARE REQUESTING SOMEONE ELSE'S INFORMATION, TO WHOM DOES IT RELATE? (Please provide their details)

Surname:	First names:
Title:	Any other names used (e.g. maiden name):
Date of birth:	
Current address: Postcode:	Previous address: Postcode:
Daytime telephone number:	
Email address:	

Your relationship to this person (please tick the relevant box)

- Mother ☐
- Father ☐
- Carer ☐
- Other (please explain below) ☐

*****You will be asked to provide proof of entitlement to request information on someone else's behalf.

Please see the Guidance Notes attached.

4. DETAILS OF THE INFORMATION YOU ARE REQUESTING:

Please describe the type of information you want to see:

Which people do you think hold the information you are requesting:

5. PROOF OF IDENTIFICATION AND ENTITLEMENT

Documents provided as proof of identity (please see the Guidance Notes):

- Passport or photo ID driving licence ☐
- Birth certificate ☐
- Bank statement ☐
- Recent utility bill (original, less than 3 months old) ☐
- Change of name documents (original) ☐

Payment:

Please enclose a cheque for £10 made payable to XXX School/Academy. The completed application form, fee and supporting proof of identity should be taken in or sent to the School.

Signature of applicant:	Date:

Subject Access Request Guidance Notes

1. **Personal Details:** Please complete your personal details as requested. Please tell us if you have been known by any other name and if you have lived at your previous address for less than two years please provide your previous address. If you are requesting historical information, then provide as many details as possible, for example previous addresses with dates. Use a separate sheet of paper if required.

2. **Details of the information you require:** You should give as much detail as possible about the information you want us to provide and the people you think might hold the information to assist us in our data search.

3. **Proof of identification:** Proof of name and address is required to ensure we only give information to the correct person. We require two original pieces of documentation, e.g. a recent utility bill (less than three months old) or a bank statement showing your name *and* address and an original piece of photo documentation such as a passport or photo ID driving licence. If you have changed your name please provide proof of this. All documents must be originals, photocopies will not be accepted.

4. **Keep your documents secure:** Documents may be brought into school or sent to us in the post. Always send these important original documents by Recorded, Special or Registered post. The school cannot be held liable for any documents lost in the post.

5. **Proof of entitlement**: Under the Data Protection Act, only the data subject has the right to ask to see their own records. All individuals aged 16 or over should make their own subject access requests if they have the mental capacity to make their own decisions (in this context mental capacity is defined as in the Mental Capacity Act 2005) unless they appoint someone else to make the request on their behalf.

6. **Making a request on behalf of someone else:** People making subject access requests on behalf of someone else need to demonstrate that they have the right to do so and we have listed the categories and proof required below. *****Please note that if you make a subject access request on behalf of a child or young person aged 12 to 15 years old, we may independently seek their consent to release the documents to you, even if you have parental responsibility for them. This means we may not disclose the information to you if they refuse their consent.

7. **A birth parent making a subject access request on behalf of their child aged below 16 years:**

   - **Birth mother:** Child's birth certificate.

   - **Birth father (married to the birth mother of the child):** Child's birth certificate and birth parent's marriage certificate.

   - **Birth father (unmarried to the birth mother of the child) for children born before 1 December 2003:** Child's birth certificate showing registration or re-registration of the birth after 1 December 2003 naming the birth father as the child's father **or** Parental Responsibility Order granted by Court **or** Residence Order granted by Court **or** proof of being appointed the child's Guardian by Court, by child's birth mother or other Guardian **or** Parental Responsibility Agreement with the birth mother.

- **Birth father (unmarried to the birth mother of the child) for children born after 1 December 2003:** Child's birth certificate naming the birth father **or** Parental Responsibility Order granted by Court **or** Residence Order granted by Court **or** proof of being appointed the child's Guardian by Court, by child's birth mother or other Guardian **or** Parental Responsibility Agreement with the birth mother.

8. An adoptive parent making a subject access request on behalf of their child aged below 16 years:

- The Adoption Order

9. A person who is not the child's parent making a subject access request on behalf of their child aged below 16 years:

- Residence Order granted by the Court **or**
- Special Guardianship Order granted by the Court **or**
- Proof of permission to make the subject access request, a signed letter or consent form from a person with parental responsibility and/or the child if the child is 12 years or older

10. A person making a subject access request on behalf of a person aged 16 years or over:

- We require proof of permission to make the request on their behalf, such as a signed letter or consent form from the person. We may contact the person for confirmation that we can release the information to you.

11. A person making a subject access request on behalf of a person lacking mental capacity aged 16 years or over:

- For a young person aged 16 – 17 years old we require proof of parental responsibility, as given in sections 5 and 6, or if you are a carer as in section 7 we require a Residence Order granted by the Court or a Special Guardianship Order granted by the Court.

- For persons aged 18 or over we require proof of a valid Lasting Power of Attorney **or** an Enduring Power of Attorney **or** proof of a Court appointed Deputyship.

12. Payment: A search fee of £10.00 is required for each separate request, an additional £10.00 fee may be charged if more than one person's records are requested. The fee is not refundable if the search shows that there is no information to be supplied. Please make all cheques payable to the school.

Appendix 2

Retention periods recommended by The Information Commissioner

Type of Document	Retention Period
Application form	Duration of employment
References received	1 year
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, eg name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

Appendix 3

Disclosure and Barring Service Advice

(adapted from…) **Advice on Handling of DBS certificate information**

(with regards to…) **Secure storage, handling, use, retention and disposal of DBS certificates and certificate information**

Storage and access - DBS disclosure information must not be stored on an employee's personnel file but should be stored separately in lockable storage with access limited to those who are entitled to see it as part of their duties.

Handling – DBS disclosure information can only be released to those who are authorised to receive it in the course of their duties. A record should be maintained of all those to whom disclosure information has been revealed. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

Usage - DBS disclosure information is only to be used for the specific purpose for which it was requested and for which the applicant's full consent will have been obtained.

Retention - Once a recruitment (or other relevant) decision has been made, DBS disclosure information should not be stored for longer than is necessary. This is generally for a period of up to six months to allow for consideration and resolution of any disputes or complaints. If, in exceptional circumstances, it is considered necessary to keep such information for longer than six months, full consideration must be given to the Data Protection rights of the individual.

Disposal - Once the retention period has elapsed, the organisation (eg school) must ensure that any DBS disclosure information is destroyed and that, whilst awaiting destruction, DBS disclosure information must be kept securely. A record of the date of issue of a disclosure, the name of the subject, the type of disclosure requested, the position for which the disclosure was requested, the unique reference number of the disclosure and the details of the recruitment decision taken should, however, be securely stored (this may be indefinitely) for monitoring purposes