Whitmore Park Primary School

Data Protection: Records Management Policy

Owner:	School Business Manager / DPO	Published date:	April 2020
Approved by Headteacher:	Jacqueline McGibney	Date:	June 2020
Approved by Chair of Governors:	Deb Austin	Date:	July 2020
Date to be reviewed:	April 2021		

Contents

1. Statement of intent and Application

Whitmore Park Primary School is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible by the appropriate individuals. In line with the requirements of the GDPR, the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, and retained in order to meet the school's statutory requirements.

This policy applies to all employees, volunteers and visitors who are privy to personal data within Whitmore Park Primary School.

The Policy applies to all records created by staff and contractors in the course of their work and includes all types such as: files, papers, maps, plans, non-standard paper documents, as well as electronic records in all formats including: computer files, email and databases, video, audio and CCTV recordings. It also applies to all records held on MIS systems and processor systems.

This Policy must be read in conjunction with the School's existing policies and procedures. Those who are not held to the Staff Code of Conduct will be asked to

return any personal data /records used in the course of their time at the school and will be prevented from further accessing records.

2. Legal framework

1.1 This policy has due regard to legislation including, but not limited to, the following:
- General Data Protection Regulation 2016
- Data Protection Act 2018
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

1.2 This policy also has due regard to the following guidance:
- Information Records Management Society (2016) 'Information Management Toolkit for Schools'
- DfE (2018) 'Data protection: a toolkit for schools'

1.3 This policy will be implemented in accordance with the following school policies and procedures:
- Data Protection Policy
- Record Retention Schedule
- CCTV Policy
- Acceptable Use Policy

3. Responsibilities

3.1 The school as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

3.2 The Governing Body and the Data Protection Officer (DPO) holds overall responsibility for the wording of this policy.

3.3 The Senior Leadership team holds overall responsibility for the implementation of this policy.

3.4 All staff are responsible for the management of records and compliance with this policy at Whitmore Park Primary School.

3.5 The Data Protection Officer is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the Governing Body and Senior Leadership Team.

3.6 All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3.7 Wherever possible, the school should promote the electronic storage of personal data.

4. Management of pupil records

4.1 Pupil records are specific documents that are used throughout a pupil's time in the education system. They are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home

address, as well as their progress and achievement.

4.2 Electronic and paper records include the following information stored in the pupil record (this is not exhaustive):

- Forename, surname, gender and date of birth
- Unique pupil number
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate
- Ethnic origin, religion and first language (if not English)
- Any preferred names
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of parents, including their home address(es) and telephone number(s)
- Name of the school, admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, e.g. speech and language therapist
- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Fair processing notice – only the most recent notice will be included
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil
- Any information about an education, health and care (EHC) plan and support offered in relation to the EHC plan
- Any notes indicating child protection disclosures and reports are held
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes indicating that records of complaints made by parents or the pupil are held

4.3 Hard copies of disclosures and reports relating to child protection are stored in a secure location– a note indicating as such is marked on the pupil's file.

4.4 Hard copies of complaints via the complaint procedure made by parents or pupils are stored securely.

4.5 Actual copies of accident and incident information are stored securely and held in line with the school's retention periods. For serious and reportable accidents, a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

4.6 Electronic records relating to a pupil's record will also be transferred to the pupils' next school in accordance with the Guidance on the Retention and Transfer of Child Protection Records and Transfers of Pupil Files to Secondary Schools in Annex A.

4.7 The school will not keep any copies of information stored within a pupil's

record, unless there is ongoing legal action at the time during which the pupil leaves the school. This excludes the personal data the school is legally required to retain. The responsibility for these records will then transfer to the next school that the pupil attends. If a child attends a school abroad or is to be home educated, the pupil file will be retained until the pupil reaches the age of 25 years.

4.8 The school will refer and adhere to the Guidance on the Retention and Transfer of Child Protection Records and Transfers of Pupil Files to Secondary Schools when a transfer of records occurs.

5. Retention of records

5.1 The School refers and adheres to its Record Retention Schedule available here.

https://www.whitmorepark.org/policies-procedures/

6. Identifying information

6.1 Under the GDPR, data controllers must apply data protection by design and default. As the data controller, the school ensures appropriate measures are in place in order for individuals to exercise their rights.

6.2 Wherever possible, the school uses pseudonymisation, also known as the 'blurring technique', to reduce the risk of identification.

6.3 Once an individual has left the school, if identifiers are no longer required, these are made less specific wherever possible and as far as is possible.

6.4 Where data is required to be retained over time, e.g. attendance data, the school removes any personal data not required and keeps only the data needed; for example, the statistics of attendance rather than personal information.

7. Storing and protecting information

7.1 The School will conduct a back-up of information routinely to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

7.2 Where possible, backed-up information will be stored off the school premises, using a central back-up service.

7.3 Confidential paper records are kept in a secure location with restricted access.

7.4 Confidential paper records are not left unattended or in clear view when held in a location with general access.

7.5 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up.

7.6 Where data is saved on removable storage or a portable device, the device is kept securely, for example in a lockable drawer when not in use.

7.7 Memory sticks are not to be used for the storage of personal data, staff should utilise the OneDrive facility instead.

7.8 All electronic devices are password-protected to protect the information on the device in case of theft.

7.9 Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

7.10 School devices are governed by the Acceptable Use Policy.

7.11 All members of staff are provided with their own secure login and password to devices and systems that access personal data under the school's control. The password must be a combination of both letters, numbers and symbols for maximum security.

7.12 External emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email or over the phone.

7.13 Circular emails to parents and those external to the school are sent blind carbon copy (bcc), including when sent from a processor's software, to ensure email addresses are not disclosed to other recipients.

7.14 Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with Data Protection Legislation, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices secure. The person taking the information from the school premises accepts full responsibility for the security of the data.

7.15 Before sharing data, staff always ensure that:

- There is a valid legal basis for sharing the data (for example, there is a safeguarding need, or consent has been obtained).
- Adequate security is in place to protect it when it is shared.
- The data recipient has been outlined in a privacy notice.
- It is not shared outside the EEA without the appropriate safeguards in place.
- A compliant contract is in place when sharing with a processor.

7.16 All staff members will implement a 'clear desk policy' wherever possible, to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored securely.

7.17 Under no circumstances are visitors allowed access to confidential or personal information without confirmation from the Head Teacher. Visitors to areas of the school containing sensitive information are supervised at all times. The confidentiality statement should be signed by volunteers.

7.18 The physical security of the school's buildings and storage systems, and access to them, is reviewed by the School's authorised personnel. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Senior Leadership Team and extra measures to secure data storage will be considered.

7.19 The school takes its duties under Data Protection Legislation seriously and any unauthorised disclosure may result in disciplinary action. This is inclusive of employees, contractors and agents who have no lawful bases for viewing/processing the personal data.

7.20 The Senior Leadership Team is responsible for continuity and recovery measures are in place to ensure the security of protected data.

7.21 Any damage to or theft of data will be managed in accordance with the school's Breach Procedure.
7.22 Personal data in relation to staff will be retained for the current academic year plus six years will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with section 7 of this policy.
7.23 Unencrypted memory sticks will never be used to store personal data.
7.24 The School will review new and existing storage methods annually and, where appropriate, discuss with the Data Protection Officer.

8. Accessing information

8.1 Whitmore Park Primary School is transparent with data subjects, the information we hold and how it can be accessed.
8.2 All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:
- Know what information the school holds and processes about them or their child and why.
- Understand their rights as individuals.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the GDPR.

8.3 All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.
8.4 The disclosure of records is limited to the specific information required to be disclosed to authorised parties and always in accordance and with strict adherence to the Data Protection Act 2018 and General Data Protection Regulation 2016.
8.5 Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information may still be shared with parents.
8.6 Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.
8.7 The school will adhere to the provisions outlined in the school's Data Protection Policy and Subject Access Request Guidance when responding to requests seeking access to personal information.

9. Mapping process

9.1 The school conducts information reviews as and when against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This is called 'data mapping' and the spreadsheet document includes a

record of the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Video and photographic records

9.2 The data mapping may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

9.3 The School's authorised personnel is responsible for completing the data mapping. The information review will include the following:

- The school's data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Who is responsible for the data asset
- Who is responsible for maintaining the original document

9.4 The School's authorised personnel will consult with staff members involved in the mapping process to ensure that the information is accurate and up to date.

9.5 Once it has been confirmed that the information is accurate and, the School's authorised personnel will record all details on the data mapping spreadsheet.

9.6 The information displayed on the data mapping spreadsheet will be shared with the Head Teacher and DPO for approval. This will be resent as and when a change is made to the document.

10. Disposal of data

10.1 The School have implemented a Record Retention Schedule to outline when data will be destroyed/retained.

10.2 Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

10.3 Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut.

10.4 Where information has been kept for administrative purposes, the School's authorised personnel and, where necessary, the DPO, will review the information again after the retention period. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

10.5 Where information must be kept permanently, this information is exempt from the normal review procedures.

11. Monitoring and review

11.1 This policy will be reviewed on an annual basis by the DPO in conjunction with the school's Head Teacher and Governing Body. The next scheduled review date for this policy is April 2021.

11.2 Any changes made to this policy will be communicated to all members of staff and the Governing Body

12. Annex A: Guidance on the Retention and Transfer of Child Protection Records and Transfers of Pupil Files to Secondary Schools.

12.1. Retention of Child Protection Records

When child protection concerns arise, all educational establishments should maintain and retain child protection records for as long as the child continues to attend the establishment; the records should then be transferred as described below.

It is recommended that child protection records are transferred with the child and then retained until a child's 25th birthday (6 years after the subject's last contact with the education establishment).

Records should then be securely disposed of and a record of disposal kept. Paper records should be shredded and electronic records deleted.

12.2. Transfer of Child Protection Records

When children transfer from one educational establishment to another, either at normal transfer stage (e.g. from Nursery to School or from School to Further Education) or as the result of a move (e.g. to another setting within Coventry to an Independent School or to another Local Authority), and records of child protection/welfare concerns exist, these should be sent to the receiving school as soon as possible, preferably within 5 days. This transfer should be arranged separately from the main pupil file in line with DfE Guidance in 'Keeping Children Safe in Education' (September 2018). Where children are dual registered (e.g. on roll at a mainstream school, but receiving education in another establishment, such as a Short Stay School or the MET), any existing child protection records should be shared with the new establishment prior to the child starting, to enable the new establishment to risk assess appropriately.

In most cases, you should wait until a pupil has been formally accepted by a new school before transferring child protection files. It would be risky to transfer child protection files to a school where a pupil has not yet been formally accepted, according to the ICO. You need a reason to disclose personal information. If you transfer a pupil's child protection files to another school and that pupil does not then move to that school, your justification for disclosing this information no longer exists.

In order to safeguard children effectively, it is important that when a child moves to a new educational establishment, the receiving establishment is immediately made aware of any current child protection concerns, preferably by telephone prior to the transfer of records. It is important that all child protection records are transferred at each stage of a child's education, up until the age of 18, or in some cases, beyond. Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. The responsibility for transfer of records lies with the originating setting and namely with the safeguarding lead, as

the receiving setting might not otherwise know that child protection concerns exist. Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required. In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives. The onus is therefore on the originating setting to facilitate the secure transfer of records, not on the receiving setting to make contact and collect the records. Paper or electronic records containing child protection information must be transferred in the most secure method available to the establishment:

- By hand if possible;
- If paper records are posted this should be by 'signed-for' delivery;
- Electronic records must only be transferred by a secure electronic transfer mechanism or after the information has been encrypted.

Child Protection records must always be passed directly and securely to the Designated Safeguarding Lead in the receiving establishment.

12.3. Transfer Form

Whether CP files are passed on by hand, by post or electronically, written evidence of this transfer (e.g. the forms at Annex B of this document) appropriately signed and dated, should be retained by both the originating and receiving setting. It is recommended that the originating establishment keeps a copy of the form for at least three academic years after the child has been transferred.

12.4. A Child subject to a Child Protection (CP) Plan or a Child in Need

If a child is the subject of a Child Protection Plan or is a Child in Need at the time of transfer the originating establishment must speak to the Designated Safeguarding Lead of the receiving establishment giving details of the child's key Social Worker from Children's Social Care Services and ensuring the establishment is made aware of the requirements of the CP Plan. If a child subject of a CP Plan leaves an establishment and the name of the child's new education placement is unknown – the Child Protection Lead should contact the child's Social Worker to discuss how and when records should be transferred.

12.5. Storage

All child protection records are sensitive and confidential so should be kept in a secure (locked at all times) filing cabinet, separate from other education records and accessible to safeguarding leads and senior staff only.

The child's education file should be marked in some way to indicate that a child protection file exists. All staff that may need to consult a child's file should be made aware what the symbol means and to speak to the safeguarding lead if they have concerns.

Electronic Child Protection Records must be password protected with access

strictly controlled in the same way as paper records.

12.6. Receiving establishment unknown

Where records of child protection/welfare concerns have been kept and details of the receiving establishment are not known, Child Protection files should be retained by the setting and transferred to the new setting, once known, or destroyed once the retention period has expired, as detailed in the Retention section above. Schools should also inform the Local Authority's Children Missing Education Officer and use the 'Lost Pupil Database' section of the 'School to School' secure data transfer service, which can be used to track missing children and trace previous schools.

12.7. Elective Home Education

If a pupil is removed from the roll to be electively home educated and there are concerns around the pupil, the educational establishment should complete the EHE checklist form to share relevant information with the Local Authority where required. The school should retain the pupil's file until the child goes back into school. If the child does not return to school, the file should be retained by the last school attended until the child reaches the age of 25. After such time, it should be securely destroyed

12.8. Transferring information when a pupil moves between schools

When a pupil ceases to be registered at a maintained school in England, the school is legally required to send a common transfer file (CTF) and educational record to the pupil's new school. This applies to all phases and types of maintained school, including special schools and pupil referral units. Safeguarding files are to be transferred in the way described above.

12.9. Transferring information about pupils with SEN

Special educational needs (SEN) support should include planning and preparation for the transitions between phases of education.

To support transition, the school should share information with the school, college or other setting the child or young person is moving to.

Schools should agree with parents and pupils the information to be shared as part of this planning process.

This is explained in the DfE's guide to the SEND code of practice.

12.10. How to transfer pupil records securely

The CTF must be transferred in machine readable form, unless either school does not have the facilities to do so.

The educational record can be transferred in machine readable form, in paper form, or in a combination of both.

This is set out in section 9(5) of the Education (Pupil Information) (England) Regulations 2005.

12.11. Transferring records electronically

The CTF is transferred through the DfE's school-to-school (S2S) system. The system is encrypted to help ensure that pupils' personal data is transferred securely.

The DfE has published guidance on using the S2S system.

12.12. Transferring paper copies of records

When transferring paper records, the Information Commissioner's Office said you should create audit trail that details:

- How the records have been transferred
- What measures were taken to protect pupils' personal data during transfer

For example, it may be safest and easiest for a member of school staff to deliver the records by hand. If this is the case, record:

- How the records were sealed prior to transfer
- Who delivered the files, on what date and at what time
- Who received the files (including a signature)

There is nothing to prevent schools sending pupils' records by courier or post, but you need to ensure that the records are appropriately sealed to reduce the risk of envelopes opening and causing an accidental data breach.

Schools should photocopy paper pupil records and retain the copy until they have received confirmation in the form of a delivery receipt that these have been received by the new school. The copy must then be shredded and the delivery receipt retained for three academic years.

12.13. Responsibility for retaining pupil records

The CTF and pupil record need to be retained until the pupil turns 25. The school where the pupil reaches statutory school leaving age (18 years old), is responsible for keeping these records.

A primary school does not need to keep copies of any of these records unless there is ongoing legal action when the pupil leaves the school.

Examples of a transfer record slip can be found at Annex A.

The completed slips for the transfer of files should be kept for at least 12 months after the date of transfer of the pupil file.

13. ANNEX B Transfer Forms for Pupil Records

Whitmore Park Primary School

Child Protection File Record of Transfer

This file contains sensitive and confidential information regarding a pupil who has recently transferred to your school. Please pass immediately to the Designated Safeguarding Lead.

Pupil Details:

Full Name …… DOB ……

Home Address ……..

Pupil UPN …… Year Group ……

Information being transferred:

CP	CIN	TAF	LAC	General Concerns

Name of Social Worker/ Family Worker ……

Status of case ……

Originating School Details:

School Name: **Whitmore Park Primary School**

Address: **Halford Lane, Coventry, CV6 2HG**

Designated Safeguarding Lead: **Jacqueline McGibney**

Receiving School Details:

School Name ……

Address ……

Designated Safeguarding Lead ……

Transfer Details:

Delivered By: …… Role ……

Signature …… Date ……...

Received By …… Role ……

Signature …… Date ……...

If the file is not delivered by hand, the receiving school should complete their details and return a copy of this form to the Designated Safeguarding Lead at Whitmore Park Primary School. If possible please scan and email to admin@whitmorepark.org or post to the above address.

Whitmore Park Primary School

General Pupil File Record of Transfer

This file contains sensitive and confidential information regarding a pupil who has recently transferred to your school.

Pupil Details:

Full Name ……. DOB ……

Home Address ……..……..

Pupil UPN …… Year Group ……

Additional Safeguarding / Child Protection / SEN Records:

Yes	No	There is a Child Protection file which will be transferred separately to your DSL
Yes	No	There is an SEN file which will be transferred separately to your SENCO
Yes	No	There are some lower level concerns or safeguarding records included in this file (in a dedicated red folder) – these need to be passed to your DSL.

Originating School Details:

School Name: **Whitmore Park Primary School**

Address: **Halford Lane, Coventry, CV6 2HG**

Office Manager: **Joanne Davis**

Transfer Details:

Delivered by …… Role ……

Delivery method: by hand / Royal Mail signed for delivery / CCC internal envelope

Signature …… Date ……...

Receiving School Details:

School Name …….

Address …….

Contact Name …….

Received By …… Role ……

Signature …… Date ……...

If the file is not delivered by hand, the receiving school should complete their details and return a copy of this form to the Office Manager at Whitmore Park Primary School.
If possible, please scan and email to admin@whitmorepark.org or post to the above address.

Whitmore Park Primary School

Pupil SEN File Record of Transfer

This file contains sensitive and confidential SEND information regarding a pupil who has recently transferred to your school. Please pass to your SENCO immediately.

Pupil Details:

Full Name …… DOB ……

Home Address ……..……..

Pupil UPN …… Year Group ……

SEN Details:

Current SEN status: ……

Originating School Details:

School Name: **Whitmore Park Primary School**

Address: **Halford Lane, Coventry, CV6 2HG**

SENDCo: **Sam Carney**

Receiving School Details:

School Name …….

Address …….

SENCO …….

Transfer Details:

Delivered By: …… Role ……

Signature …… Date ……...

Received By …… Role ……

Signature …… Date ……...

If the file is not delivered by hand, the receiving school should complete their details and return a copy of this form to the SENDCo at Whitmore Park Primary School.

If possible please scan and email to admin@whitmorepark.org or post to the above address.