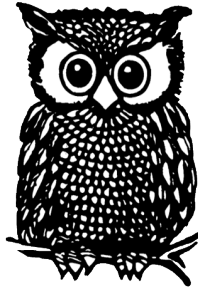


Metheringham Primary School



DATA PROTECTION POLICY

Metheringham Primary School,
Princes Street,
Metheringham,
Lincoln,
LN4 3BX
Tel 01526 320039

Email: enquiries@metheringham.lincs.sch.uk

www.metheringhamprimary.co.uk

1. Introduction

- 1.1. Metheringham Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is processed in order to enable the School to provide education and other associated functions. In addition, there may be a legal requirement for the School to process personal information to ensure that it complies with statutory obligations.
- 1.2. Schools have a duty, as Data Controllers, to keep detailed records of data processing activities and the records shall contain:-
 - Name and details of the organisation (and where applicable, of other controllers, any representative and data protection officer)
 - Purposes of the processing
 - Description of the categories of individuals and categories of personal data.
 - Categories of recipients of personal data
 - Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
 - Retention schedules
 - Description of technical and organisational security measures

These records must be made available to the Information Commissioner's Office (ICO) upon request. The School will, on an annual basis, provide its registrable particulars and pays the data protection fee to the ICO.

2. Purpose

- 2.1. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR and DPA and other related legislation. It will apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.
- 2.2. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall attend regular training to ensure compliance with their responsibilities.

3. Key principles

- 3.1 Personal information or data is defined as any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier held by the school.
 - 3.1.1 Data Protection Principles – there are six enforceable principles contained in Article 5 of the General Data Protection Regulations. They are key to compliance and the School must endeavour to ensure that they are adhered to at all times. The responsibility for adherence to the principles is the responsibilities of all School staff.
 - 3.1.2 Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
 - 3.1.3 Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
 - 3.1.4 Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary.
 - 3.1.5 Principle 4 – Personal data shall be accurate and where necessary, kept up to date. Steps must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
 - 3.1.6 Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
 - 3.1.7 Principle 6 - Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

3.2 To ensure compliance with the above principles the School will:

- (a) Produce an information asset register that contains details of the records it holds.
- (b) Inform individuals why the information is being collected at the point it is collected by way of privacy notices.
- (c) Inform individuals when their information is shared, and why and with whom it will be shared.
- (d) Check the quality and the accuracy of the information it holds.

- (e) Ensure that information is not retained for longer than is necessary.
- (f) Ensure that when obsolete information is destroyed and it is done so appropriately and securely.
- (g) Create, maintain and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.
- (h) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- (i) Share information with others only when it is fair and lawful to do so and satisfies the lawful basis for processing that information.
- (j) Share personal data with other organisations for the purpose of crime prevention and/or detection, or for the purpose of legal proceedings, provided that the disclosure falls within an exemption to the non-disclosure provisions contained within the Data Protection Act 1998 or any subsequent legislation.
- (k) Disclose personal data where required to do so by law for example, following receipt of a court order.
- (l) Set out procedures to ensure compliance with the duty to respond to an individual's rights to:
 - request access to personal information, known as Subject Access Requests.
 - be informed about the way their data is used;
 - have inaccurate personal data rectified;
 - have their personal data erased;
 - restrict the processing of their personal data; and
 - object to the processing of their personal data.
- (m) Ensure our staff are appropriately and regularly trained and aware of and understand our policies and procedures.
- (n) Create and maintain a data breach notification spreadsheet to record data breaches and also circumstances where a breach was narrowly avoided.

4. Data Protection Officer (DPO)

4.1 The Data Protection Officer – our DPO is Judy Carter and can be contacted on 01526 343180 / 07834690101

- 4.2 The DPO cannot hold a position that requires them to determine the purpose and means of processing personal data, for example, the Head Teacher, head of human resources, or head of information technology.

5. Data Protection Impact Assessments (DPIA)

- 5.1 The School must carry out a DPIA when processing is likely to result in **high risk** to the rights and freedoms of individuals.
- 5.2 The GDPR does not define high risk but guidance highlights a number of factors that are likely to trigger the need for a DPIA, which include the use of new technologies, processing on a large scale, systematic monitoring, processing of special categories of personal data.

6. Privacy Notices

- 6.1 The School publishes a privacy notice on its website which provides information about how and why the school gathers and uses images and shares personal data.
- 6.2 The privacy notice under the GDPR should include:
- Who you are and how they can contact you;
 - The personal data you are collecting & why you are collecting it;
 - Where you get the personal data from & who you are sharing it with;
 - How long the data will be held for;
 - Transfers to third countries and safeguards;
 - Description of the data subjects individual rights;
 - The data subjects right to withdraw consent for the processing of their data; and
 - How individuals can complain.
- 6.3 The privacy notice will be reviewed at regular intervals to ensure it reflects current processing.
- 6.4 The privacy notice will be amended to reflect any changes to the way the School processes personal data.
- 6.5 Whilst the School will publish an overarching privacy notice it will also issue a privacy notice to all parents and pupils, before, or as soon as possible after, any personal data relating to them is obtained. This may simply be an explanation why the information is being requested and the purpose for which it will be used.
- 6.6 The privacy notice will include details of how the School uses CCTV, whether it intends to use biometric data and how consent will be requested to do this and include details of the School's policy regarding photographs and electronic images of pupils.

7 Close Circuit Television (CCTV)

- 7.5 Images and audio recordings of identifiable individuals captured by Closed Circuit Television amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by the General Data Protection Regulations and the Data Protection Act as other types of recorded information.
- 7.6 The School will use CCTV for the following purposes:
- To protect the school buildings and assets;
 - To increase personal safety of staff, pupils and visitors;
 - To reduce the fear of crime;
 - To support the Police in order to deter and detect and to apprehend and prosecute offenders;
 - To help protect members of the public and private property;
 - To investigate both pupil and staff behaviour where appropriate.
- 7.7 The School will ensure that any use of CCTV is necessary and proportionate to achieve the aims stated in 7.6 and will ensure that regular reviews of the use of CCTV within the School take place.
- 7.8 The School will ensure that any use of CCTV is included in its records of data processing activity.
- 7.9 The School's use of CCTV will comply with the Information Commissioner's Office CCTV Code of Practice <https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/> .
- 7.10 The School will ensure that clear notices are in place identifying when an individual is entering an area that is monitored by CCTV. The notice will identify the School as the responsible data controller and will state the purpose for which the recording is taking place.
- 7.11 The School will not operate audio recording as part of the CCTV without seeking additional advice.
- 7.12 The School will not operate CCTV in any areas of the premises where individuals would have a legitimate expectation of personal privacy, such as toilets or changing rooms.
- 7.13 The School will ensure that CCTV recordings are kept securely and that access to them is restricted to those staff that operate the system or make decisions relating to how the images should be used.
- 7.14 Retain in line with the retention schedule.

8 Photographs and Electronic Images

- 8.1 The School has developed a Social Media Policy in relation to the use of photographs/videos that contain images of pupils. The policy provides the School's position regarding parents photographing and filming pupils at school events and the use of images of pupils by the School in any School publicity material, its website, in newspapers and in outside agency publications.

9 Biometric Data

- 9.1 If the School uses or intends to use biometric data (such as fingerprint technology) a separate, detailed notice will be sent to all pupils and parents explaining the intended reasons for and lawful basis for the use of the data, and provide parents with options for alternative systems if they do not wish their child to provide this information and want to opt out.
- 9.2 The School will obtain the written consent of at least one parent or carer with Parental Responsibility for the child before taking and using any biometric data from a pupil.
- 9.3 Metheringham Primary School currently does not use any form of biometric data.

10 Requests for Access to Personal Data

- 10.1 This section sets out the process that will be followed by the school when responding to requests for access to personal data made by the pupil or their parent or carer with Parental Responsibility.
- 10.2 There are two distinct rights of access to information held by schools about pupils, parents/carers and staff:
- (a) Pupils have a right to make a request under the GDPR to access the personal information held about them.
 - (b) Pupils and parents or those with Parental Responsibility have a right to access the educational records. The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005.
- 10.3 Handling a subject access request for access to personal data:
- 10.3.1 Article 15 of the GDPR gives individuals the right to access personal data relating to them, processed by a data controller. The right can be exercised by a person with Parental Responsibility on behalf of their child dependent on the age and the understanding of the child. For the purposes of a subject access request the school will apply the full legal definition of 'Parental Responsibility' when determining who can access a child's personal data.

- 10.3.2 Requests for information must be made in writing; which can include e-mail, and be addressed to the Head Teacher or the Chair of Governors. If the original request does not clearly identify the information required, then the School will seek further enquiries to clarify what information is being requested.
- 10.3.3 The identity of the requestor must be established before the disclosure of any information is made. Proof of the relationship with the child (if not known) must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child. Below are some examples of documents which can be used to establish identity:
- Passport
 - Driving licence
 - Utility bill with current address
 - Birth/marriage certificate
 - P45/P60
 - Credit card or mortgage statement.
- 10.3.4 It is widely accepted that children of primary school age do not have the maturity to understand and exercise their own rights and as such it is acceptable for those with Parental Responsibility to exercise these rights on their child's behalf. However, each request will be considered on its own merits and the circumstances surrounding the request and the child. A child with competency to understand can refuse to consent to a request for their personal information made under the GDPR. This position differs when the request is for access to the Education Record of the child (see below for more detail).
- 10.3.5 No charge can be made for access to personal data that is not contained within an education record.
- 10.3.6 The response time for a subject access request is one month from the date of the request (irrespective of school holiday periods). The one month period will not commence until any necessary clarification of information is sought. The time to respond can be extended to two months where the request is complex or numerous.
- 10.3.7 There are some exemptions available under the Data Protection Act which will mean that occasionally personal data will need to be redacted (information blacked out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosure to ensure that the intended disclosure complies with the School's legal obligations.
- 10.3.8 Where the personal data also relates to another individual who can be identified from the information, the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the

subject of the request, consideration will be given to withholding the information from disclosure. These considerations can be complex and additional advice will be sought when necessary.

- 10.3.9 Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another person will be withheld along with any information that would reveal that the child is at risk of abuse, or information relating to Court Proceedings.
 - 10.3.10 Where redaction has taken place then a full copy of the information provided will be retained in order to maintain a record of what was redacted and why and a clear explanation of any redactions will be provided in the School's response to the request.
 - 10.3.11 If there are concerns about the disclosure of information additional advice will be sought.
- 10.4 Handling a request for access to a curricular and educational record as defined within the Education (Pupil Information) (England) Regulations 2005.
- 10.4.1 A parent may make a request to access information contained within their child's education record, regardless of whether the child agrees to the disclosure of information to them. The right of access belongs to the parent in these cases. It is not a right being exercised by the parent on behalf of the child.
 - 10.4.2 For the purpose of responding to an Educational Records request, the School will apply the definition of 'parent' contained within the Education Act 1996.
 - 10.4.3 An "educational record" means any record of information which-
 - a. Is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local education authority and any special school which is not so maintained.
 - b. Relates to any person who is or has been a pupil at any such school; and
 - c. Originated from or was supplied by or on behalf of the persons specified in paragraph (a), other than information which is processed by a teacher solely for the teacher's own use
 - 10.4.4 The amount that can be charged for a copy of information contained in an education record will depend upon the number of pages provided. The charge made will be in accordance with the Education (Pupil Information) (England) Regulations 2005.
 - 10.4.5 No charge will be made to view the education record.

- 10.4.6 The response time for requests made under the Education (Pupil Information) (England) Regulations 2005 is 15 school days (this does not include half terms or teacher training days).
- 10.4.7 An exemption from the obligation to comply with the request will be claimed where the disclosure of the information to the parent may cause serious harm to the physical or mental or emotional condition of the pupil or another person or if the disclosure of the information would reveal that the child is at risk of abuse.
- 10.4.8 If a subject access request is made for information containing in whole or in part a pupils educational record a response must be provided within 15 school days

11. Retention and Disposal of personal data

- 11.1 The Governing Body of the School will ensure that the School has an up to date and accurate retention and disposal schedule that is compliant with the GDPR. The School will ensure that personal data is stored, transferred and disposed of securely and in accordance with the retention and disposal schedule.

12. Security of personal data

- 12.1 The School will ensure that appropriate security measures are in place and enforced to keep paper and electronic personal data secure.
- 12.2 The School will regularly review the physical security of the School buildings and storage systems.
- 12.3 The School will ensure that only authorised individuals have access to personal data.
- 12.4 All portable electronic devices containing personal data will be encrypted.
- 12.5 No personal data will be left unattended in any vehicles and staff will ensure that if it is necessary to take personal data from School premises, for example to complete work from home, the data is suitably secured.
- 12.6 The School will refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud based solution.

13. Complaints

- 13.1 Complaints relating to the School's compliance with the GDPR will be dealt with in accordance with the school's complaint policy.

- 13.2 Complaints relating to access to personal information or access to education records should be made to Mrs Leanne Duggin, Headteacher, who will decide whether it is appropriate for the complaint to be dealt with through the School's complaints procedure. Complaints which are not appropriate to be dealt with through the school's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter. [Reference to the ICO should only usually be made where the Schools internal complainants' process has been exhausted]
- 13.3. Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 01625 5457453

14. Review

- 14.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. The policy review will be undertaken by the Head teacher or nominated representative.

15. Contacts

- 15.1 If you have any enquiries in relation to this policy, please contact the Headteacher on 01526 320039 or at enquiries@metheringham.lincs.sch.uk
- 15.2 Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk or telephone 01625 5457453

Appendix A: Annual review of school records and safe data destruction checklist

Metheringham Primary School

Completion page

School name: Metheringham Primary School

Review completed by:

Date:

Approved by Headteacher:

Date:

Note – The completion of this review should be shared at the Governors meeting and minuted.

A. Summary of areas reviewed:

Ref	Area	Pages	Annual Review Completed Tick (v)	Reviewer Initials
1	Management of the School	5 to 9		
2	Human Resources	10 to 12		
3	Financial Management of the School	13 to 14		
4	Property Management	15		
5	Pupil Management	16 to 17		
6	Curriculum Management	18		
7	Extra-Curricular Activities	19 to 20		

8	Central Government and Local Authority	21		
9	List of School Records and Data safely destroyed	22		

A. Aims

This checklist has been produced based on the “Information Management Toolkit for Schools” (IMTIS) dated 1 February 2016 and developed and published by the Information Record Management Society (“IRMS”).

This checklist has been produced in accordance with the guidance produced by the DFE in April 2018 in the “GDPR Toolkit for Schools” and is in accordance with the Data Protection rules and Freedom of Information Act (2000) legislation.

This is a checklist developed to enable School Business Managers, Clerks, SENCO and other School Staff to carry out an efficient annual review and safe destruction of school records and information.

Where there is legal statute behind a requirement this is detailed in the IMTIS document.

B. Safe Destruction of Data

(i) Disposal of records that have reached the end of the minimum retention period allocated

The fifth data protection principle as per the data protection rules (updated for GDPR) states that:

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

In each school, the leadership must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

The school review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the school for research or litigation purposes.

Whatever decisions are made they need to be documented as part of the records management policy within the school.

(ii) Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

- a) Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

- b) Where records are destroyed internally, the process must ensure that all records are recorded and authorised to be destroyed by a member of the Leadership team and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

(iii) [Freedom of Information Act 2000 \(FoIA 2000\)](#)

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction

Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range
- The name of the authorising officer
- Date action taken

Following this guidance will ensure that the school is compliant with the Data Protection rules and the Freedom of Information Act 2000.

If you have any queries in completing this checklist please contact:

The Data Protection Officer
The Oxford Diocesan Schools Trust
Church House Oxford
Langford Locks
Kidlington
Oxford OX5 1GF

Email: dpo.odst@oxford.anglican.org

Phone: 01865 208 200

Version Control History: First Edition – June 2018

1. Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff	One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL ^{L11}	
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)		PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service	
	Inspection Copies ^{L21}		Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.	
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff	Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes	
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL	

1.1 Governing Body (continued...)					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the	Annual Review Completed

				administrative life of the record	Tick (v)
1.1.5	Instruments of Government including Articles of Association	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.	
1.1.6	Trusts and Endowments managed by the Governing Body	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.	
1.1.7	Action plans created and administered by the Governing Body	No	Life of the action plan + 3 years	SECURE DISPOSAL	
1.1.8	Policy documents created and administered by the Governing Body	No	Life of the policy + 3 years	SECURE DISPOSAL	
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes	Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL	
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Date of report + 10 years	SECURE DISPOSAL	
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No	Date proposal accepted or declined + 3 years	SECURE DISPOSAL	

1.2 Head Teacher and Senior Management Team					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
1.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff	Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate	
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff	Date of the meeting + 3 years then review	SECURE DISPOSAL	
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff	Date of the report + a minimum of 3 years then review	SECURE DISPOSAL	
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff	Current academic year + 6 years then review	SECURE DISPOSAL	
1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff	Date of correspondence + 3 years then review	SECURE DISPOSAL	
1.2.6	Professional Development Plans	Yes	Life of the plan + 6 years	SECURE DISPOSAL	
1.2.7	School Development Plans	No	Life of the plan + 3 years	SECURE DISPOSAL	

1.3 Admissions Process					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	Life of the policy + 3 years then review	SECURE DISPOSAL	
1.3.2	Admissions – if the admission is successful	Yes	Date of admission + 1 year	SECURE DISPOSAL	
1.3.3	Admissions – if the appeal is unsuccessful	Yes	Resolution of case + 1 year	SECURE DISPOSAL	
1.3.4	Register of Admissions	Yes	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made. ³	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.	
1.3.5	Admissions – Secondary Schools – Casual	Yes	Current year + 1 year	SECURE DISPOSAL	
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	Current year + 1 year	SECURE DISPOSAL	
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions		This information should be added to the pupil file	SECURE DISPOSAL	

	For unsuccessful admissions		Until appeals process completed	SECURE DISPOSAL	
--	-----------------------------	--	---------------------------------	-----------------	--

1.4 Operational Administration					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
1.4.1	General file series	No	Current year + 5 years then REVIEW	SECURE DISPOSAL	
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No	Current year + 3 years	STANDARD DISPOSAL	
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No	Current year + 1 year	STANDARD DISPOSAL	
1.4.4	Newsletters and other items with a short operational use	No	Current year + 1 year	STANDARD DISPOSAL	
1.4.5	Visitors' Books and Signing in Sheets	Yes	Current year + 6 years then REVIEW	SECURE DISPOSAL	
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No	Current year + 6 years then REVIEW	SECURE DISPOSAL	

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
2.1.1	All records leading up to the appointment of a new headteacher	Yes	Date of appointment + 6 years	SECURE DISPOSAL	
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes	Date of appointment of successful candidate + 6 months	SECURE DISPOSAL	
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes	All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL	
2.1.4	Pre-employment vetting information – DBS Checks	No	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months		
2.1.5	Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes	Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file		
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom ⁴	Yes	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years		

2.2 Operational Staff Management					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
2.2.1	Staff Personal File	Yes	Termination of Employment + 6 years	SECURE DISPOSAL	
2.2.2	Timesheets	Yes	Current year + 6 years	SECURE DISPOSAL	
2.2.3	Annual appraisal/ assessment records	Yes	Current year + 5 years	SECURE DISPOSAL	

2.3 Management of Disciplinary and Grievance Processes					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded ⁵	Yes	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded	
2.3.2	Disciplinary Proceedings	Yes			
	oral warning		Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]	
	written warning – level 1		Date of warning + 6 months		
	written warning – level 2		Date of warning + 12 months		

	final warning		Date of warning + 18 months		
	case not found		If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL	

2.4 Health and Safety					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
2.4.1	Health and Safety Policy Statements	No	Life of policy + 3 years	SECURE DISPOSAL	
2.4.2	Health and Safety Risk Assessments	No	Life of risk assessment + 3 years	SECURE DISPOSAL	
2.4.3	Records relating to accident/ injury at work	Yes	Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL	
2.4.4	Accident Reporting	Yes			
	Adults		Date of the incident + 6 years	SECURE DISPOSAL	
	Children		DOB of the child + 25 years	SECURE DISPOSAL	
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Current year + 40 years	SECURE DISPOSAL	
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Last action + 40 years	SECURE DISPOSAL	
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in	No	Last action + 50 years	SECURE DISPOSAL	

	contact with radiation				
2.4.8	Fire Precautions log books	No	Current year + 6 years	SECURE DISPOSAL	

2.4 Payroll and Pensions					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
2.5.1	Maternity pay records	Yes	Current year + 3 years	SECURE DISPOSAL	
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Current year + 6 years	SECURE DISPOSAL	

3. Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals

3.1 Risk Management and Insurance					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
3.1.1	Employer's Liability Insurance Certificate	No	Closure of the school + 40 years	SECURE DISPOSAL	

3.2 Asset Management					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
3.2.1	Inventories of furniture and equipment	No	Current year + 6 years	SECURE DISPOSAL	
3.2.2	Burglary, theft and vandalism report forms	No	Current year + 6 years	SECURE DISPOSAL	

3.3 Accounts and Statements including Budget Management					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
3.3.1	Annual Accounts	No	Current year + 6 years	STANDARD DISPOSAL	
3.3.2	Loans and grants managed by the school	No	Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL	
3.3.3	Student Grant applications	Yes	Current year + 3 years	SECURE DISPOSAL	
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No	Life of the budget + 3 years	SECURE DISPOSAL	
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years	SECURE DISPOSAL	
3.3.6	Records relating to the collection and banking of monies	No	Current financial year + 6 years	SECURE DISPOSAL	
3.3.7	Records relating to the identification and collection of debt	No	Current financial year + 6 years	SECURE DISPOSAL	

3.4 Contract Management					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
3.4.1	All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years	SECURE DISPOSAL	
3.4.2	All records relating to the management of contracts under signature	No	Last payment on the contract + 6 years	SECURE DISPOSAL	
3.4.3	Records relating to the monitoring of contracts	No	Current year + 2 years	SECURE DISPOSAL	

3.5 School Fund

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
3.5.1	School Fund - Cheque books	No	Current year + 6 years	SECURE DISPOSAL	
3.5.2	School Fund - Paying in books	No	Current year + 6 years	SECURE DISPOSAL	
3.5.3	School Fund – Ledger	No	Current year + 6 years	SECURE DISPOSAL	
3.5.4	School Fund – Invoices	No	Current year + 6 years	SECURE DISPOSAL	
3.5.5	School Fund – Receipts	No	Current year + 6 years	SECURE DISPOSAL	
3.5.6	School Fund - Bank statements	No	Current year + 6 years	SECURE DISPOSAL	
3.5.7	School Fund – Journey Books	No	Current year + 6 years	SECURE DISPOSAL	

3.6 School Meals					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
3.6.1	Free School Meals Registers	Yes	Current year + 6 years	SECURE DISPOSAL	
3.6.2	School Meals Registers	Yes	Current year + 3 years	SECURE DISPOSAL	
3.6.3	School Meals Summary Sheets	No	Current year + 3 years	SECURE DISPOSAL	

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
4.1.1	Title deeds of properties	No	PERMANENT These should follow the property unless		

	belonging to the school		the property has been registered with the Land Registry		
4.1.2	Plans of property belong to the school	No	These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.		
4.1.3	Leases of property leased by or to the school	No	Expiry of lease + 6 years	SECURE DISPOSAL	
4.1.4	Records relating to the letting of school premises	No	Current financial year + 6 years	SECURE DISPOSAL	

4.2 Maintenance					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
4.2.1	All records relating to the maintenance of the school carried out by contractors	No	Current year + 6 years	SECURE DISPOSAL	
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No	Current year + 6 years	SECURE DISPOSAL	

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above

5.1 Pupil's Educational Record					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes			
	Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. 131	
	Secondary		Date of Birth of the pupil + 25 years	SECURE DISPOSAL	
5.1.2	Examination Results – Pupil Copies	Yes			
	Public		This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.	
	Internal		This information should be added to the pupil file		
5.1.3	Child Protection information held on pupil file		If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded	
5.1.4	Child protection information held in separate files		DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded	

5.2 Attendance					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
5.2.1	Attendance Registers	Yes	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL	
5.2.2	Correspondence relating to authorized absence		Current academic year + 2 years	SECURE DISPOSAL	

5.3 Special Educational Needs					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.	
5.3.2	Statement maintained under section 234 of the Education Act	Yes	Date of birth of the pupil + 25 years [This would normally be	SECURE DISPOSAL unless the document is subject to a legal hold	

	1990 and any amendments made to the statement		retained on the pupil file]		
			Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	
			Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	

6. Curriculum Management

6.1 Statistics and Management Information					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
6.1.1	Curriculum returns	No	Current year + 3 years	SECURE DISPOSAL	
6.1.2	Examination Results (Schools Copy)	Yes	Current year + 6 years	SECURE DISPOSAL	
	SATS records –	Yes			
	Results		<p>The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years.</p> <p>The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison</p>	SECURE DISPOSAL	
	Examination Papers		The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL	

6.1.3	Published Admission Number (PAN) Reports	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.4	Value Added and Contextual Data	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.5	Self-Evaluation Forms	Yes	Current year + 6 years	SECURE DISPOSAL	

6.2 Implementation of Curriculum

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (✓)
6.2.1	Schemes of Work	No	Current year + 1 year	Review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL	
6.2.2	Timetable	No	Current year + 1 year		
6.2.3	Class Record Books	No	Current year + 1 year		
6.2.4	Mark Books	No	Current year + 1 year		
6.2.5	Record homework set	No	Current year + 1 year		
6.2.6	Pupils' Work	No	Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL	

7. Extra Curriculum Management

7.1 Educational Visits outside the Classroom

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (✓)
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Date of visit + 14 years	SECURE DISPOSAL	
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the	No	Date of visit + 10 years	SECURE DISPOSAL	

	Classroom – Secondary Schools				
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes	Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.	
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils		

7.2 Walking Bus					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
7.2.1	Walking Bus Registers	Yes	Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]	

7.3 Family Liaison Officers and Home School Liaison Assistants					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
7.3.1	Day Books	Yes	Current year + 2 years then review		

7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes	Whilst child is attending school and then destroy		
7.3.3	Referral forms	Yes	While the referral is current		
7.3.4	Contact data sheets	Yes	Current year then review, if contact is no longer active then destroy		
7.3.5	Contact database entries	Yes	Current year then review, if contact is no longer active then destroy		
7.3.6	Group Registers	Yes	Current year + 2 years		

8. Central Government and Local Authority

8.1 Local Authority					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
8.1.1	Secondary Transfer Sheets (Primary)	Yes	Current year + 2 years	SECURE DISPOSAL	
8.1.2	Attendance Returns	Yes	Current year + 1 year	SECURE DISPOSAL	
8.1.3	School Census Returns	No	Current year + 5 years	SECURE DISPOSAL	
8.1.4	Circulars and other information sent from the Local Authority	No	Operational use	SECURE DISPOSAL	

8.2 Central Government					
Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (v)
8.2.1	OFSTED reports and papers	No	Life of the report then REVIEW	SECURE DISPOSAL	

8.2.2	Returns made to central government	No	Current year + 6 years	SECURE DISPOSAL	
8.2.3	Circulars and other information sent from central government	No	Operational use	SECURE DISPOSAL	

Appendix B – List of School Records and Data safely destroyed

The following sheet can be completed or alternatively documented in a spreadsheet.

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	<u>Confirm</u> (i) Safely destroyed (ii) In accordance with Data Retention Guidelines Tick (v)
<i>e.g.</i>	<i>School Invoices</i>	<i>Copies of purchase invoices dated 2011/12</i>	<i>Folders marked "Purchase Invoices 2011/12" 1 to 3</i>	<i>3 Folders</i>	<i>Shredding</i>	v
1						
2						
3						
4						
5						

6						
7						
8						
9						
10						
11						
12						
13						
14						

[1] In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

[2] These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

[3] This will include: (i) to another primary school (ii) to a secondary school (iii) to a pupil referral unit (iv) If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority