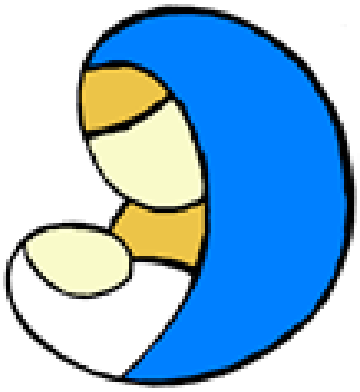
St. Mary's RC Primary School



Information Management Policy

Mission Statement: We Care, We Pray, We Work, We Play in Jesus' Way

Version / Issue No.	Date	Author	Remarks / Reason for Change
V.01	02.11.2012	Paul Rankin	
V 02	14.04.2014	Tasadiq Naveed	
V 03	05.03.2015	Tasadiq Naveed	
V 04	02/05/2018	Ann McDonna	Update policy with GDPR
V 05	01/06/2018	Imran Khan	Update policy with correct links and reference to Goddard Enquiry

Reviewed by Governors: May 2022

Reviewed: May 2024

To be reviewed: May 2026

The General Data Protection Regulation (GDPR) and the Data Protection Bill

The General Data Protection Regulation (GDPR) is a Europe-wide law which is part of a wider package of reform intended to modernise data protection laws.

The Data Protection Act 1998 was introduced to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data. GDPR builds on this legislation, enhancing information rights for the public and placing a much greater emphasis on organisations being able to show how they comply with the data protection principles, for example by having effective policies and procedures in place, and documenting and demonstrating their accountability.

GDPR applies to all personal data, regardless of whether it is held electronically (on a computer system, in emails, in text messages etc.) or on paper. There are particularly stringent rules surrounding "special category" data (similar to 'sensitive' data in the Data Protection Act 2018) such as pupil identifiers, pupil characteristics, special educational needs, health, religious beliefs, ethnic background, home address and biometric data. In addition GDPR explicitly states that children's personal data merits specific protection.

GDPR also introduces new responsibilities around the collection and use of pseudonymised personal data (data where any identifying characteristics have been replaced with a pseudonym (or value) that means that the data subject cannot be directly identified, but they can be identified by indirect means such as using underlying or related data. For example: where an individual is allocated a client reference which is used instead of their name.)

As GDPR and the Data Protection Bill complement each other it is important that they are read side by side.

St Mary's RC Primary School is registered with the Information Commissioner's Office as a Data Controller and aims to fulfil its obligations to the fullest extent and to comply with the six data protection principles set out in the GDPR which require that personal data is:

1. Processed lawfully, fairly and transparently
2. Collected for a specified, explicit and legitimate purpose
3. Adequate, relevant and limited to what is necessary (ie: proportionate) for the purpose it is being processed
4. Accurate and kept up to date, with every reasonable step taken to erase or rectify inaccurate personal data without delay
5. Held in a form that means the data subject can be identified for only as long as is necessary for the purpose for which the personal data is processed
6. Processed in a manner that ensures appropriate security of the personal data

Processing Personal Data

Before processing personal data the school will first identify a legal basis for doing so. When processing special category data the school will also satisfy one of the special category conditions.

Details of the legal bases, special categories of data and the special category conditions can be found in Appendix 1.

Privacy Notice - Fair Processing of Data

Under principle 4 of the GDPR, the school has a duty to check that children, parents and carers information is accurate and up to date. It fulfils this by sending out a data collection form to parents/carers on an annual basis. This form will also include a privacy notice which outlines to the parent/carer:

- What information is held
- Why the information is held
- How long the information is held
- Who the information is shared with
- How children, parents and carers can access the information which is held about them

The school also has a duty to check that staff information is accurate and up to date. It fulfils this by asking staff to complete a data collection form. The form will also include a privacy notice which will outline:

- What information is held
- Why the information is held
- How long the information is held
- Who the information is shared with
- How staff can access the information which is held about them

An updated privacy notice for staff data is available on the Extranet.

Consent

Consent is one of the legal bases available to the school, although this will only be used where there is no other legal basis available.

Where the school is relying on consent to process personal data, this will be proactive, made clear to the data subject and will be separate from other matters. It will also be made clear that consent can be withdrawn at any time and the method to do so will be clear and accessible; it will be as easy to withdraw consent as it was to give consent.

If consent is withdrawn, the school will immediately cease processing the personal data.

There are additional provisions within GDPR regarding securing consent from children. When offering an online service directly to a child, only children aged 13 or over are able provide their own consent. For younger children, consent would need to be provided by whoever holds parental responsibility for the child (unless the online service offered is a preventive or counselling service). In such cases, the school will make reasonable efforts to verify that consent is given or authorized by a parent or guardian.

Information Security

Under principle 6 of the GDPR, the school has a duty to ensure that data is handled securely. To fulfil its obligations under the act and to comply with Cabinet Office guidelines outlined in “Data Handling Procedures in Government” the school will adopt the following to maintain data security:

- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Sensitive or personal data must be securely deleted when it is no longer required.
- Computer passwords should not be disclosed or shared between users
- Files and paperwork that identifies individuals must never be left unattended and must be stored in locked cabinets within a controlled access room that must be locked when not in use
- All staff processing personal information should be appropriately trained

The school will use a protective marking scheme to ensure that all data – electronic or on paper – is labelled according to the protection it requires based on Impact Levels:

Impact level	Colour Code	Memory stick?	Example
IL0–Not Protectively Marked		No	Newsletters, public information
IL1- Unclassified		No	Generic letters to parents containing no personal data
IL2–PROTECT		No	Basic student information such as name and address
IL3–Restricted		No	Sensitive Student information such as ethnicity or FSM status
IL4-Confidential		No	Highly sensitive student data relating to child protection

Information Asset Register and Record of Processing Activity
An information asset register will be compiled and kept up to date. This will summarise each information asset the school maintains and include a record of activities related to higher risk processing such as processing personal data that could result in a risk to the rights and freedoms of individuals, and the processing of special category data, or criminal convictions / offences.

Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned.

The information documented in the information asset register must reflect the current situation as regards the processing of personal data and therefore will be regularly reviewed to ensure that it remains accurate and up to date.

Data Protection Impact Assessments
In order to ensure that all data protection requirements are identified and any associated risks are addressed, the school will complete a Data Protection Impact Assessment (DPIA) (previously known as a privacy impact assessment (PIA)) when introducing a new, or revising an existing, system or process which involves processing personal data.

Data Protection Officer
As a public authority, the school has a duty under GDPR to appoint a Data Protection Officer to assist with monitoring internal compliance, inform and advise on the school's data protection obligations and provide advice regarding Data Protection Impact Assessments (DPIAs).

The DPO will be independent, an expert in data protection, adequately resourced, and report to the highest management level.

Incident Reporting
GDPR introduces a legal duty to report certain types of personal data breach to the Information Commissioner's Office (ICO); this must be done **within 72 hours** of the school becoming aware of the breach, where feasible, even if all details of the breach are not yet known.

In addition, the school is required to inform the data subjects of the breach without undue delay if it is considered that there is a high risk of the breach adversely affecting their rights and freedoms.

In order to meet these requirements, any suspected and/or actual breaches of information security will be reported to the school's Data Protection Officer immediately, and in any event **within 24 hours** of the school becoming aware of the breach, using the form attached at Appendix 3.

Records will be maintained of any suspected breaches of information security using this form. The details of the incident will be used to determine whether the breach requires a report to the ICO and/or the data subjects, and, following investigation, to create a correctional plan to ensure that a similar incident does not happen.

Record Retention
The school maintains a records management policy which details compliance with the Lord Chancellor's Code of Practice which can be found here:
http://webarchive.nationalarchives.gov.uk/20150603223501/https://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf

A detailed retention schedule and protective marking scheme is outlined in Appendix 2

This retention schedule is based on guidance from the records management society:
https://cdn.ymaws.com/irms.org.uk/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

It encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

**Please note that retaining documents beyond their retention or transfer dates may breach principle 5 of GDPR

The Right to be Forgotten

Under GDPR individuals have the right to have personal data erased, this is also known as the 'right to be forgotten'. There is a particular emphasis on the right to erasure if the request relates to data collected from children. The right to be forgotten is not absolute and only applies in certain circumstances.

An individual can make a request for data to be erased either verbally or writing. The school will respond to such requests within 1 calendar month to advise of its decision and will provide a clear justification if it refuses the request.

If personal data which the school has shared with others is erased, the school will inform each recipient of the erasure, unless this proves impossible or involves disproportionate effort.

Disclosure of personal information
Personal information will be disclosed to 3rd parties under the following conditions:

Information sharing with professionals working with children
Information sharing between professionals is vital to ensure the wellbeing of Children. The school will follow the "7 Golden Rules of Information Sharing" described by the DfE:

1. Remember that GDPR is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate
5. Consider safety and well-being

6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277834/information_sharing_guidance_for_practitioners_and_managers.pdf

Unauthorised disclosure of personal data is a criminal offence under Section 55 of the Data Protection Act 1998 and will likely lead to disciplinary action

Investigation of a crime

As Data Controller personal data can be shared with the police and Crown Prosecution Service (CPS) so long as it is about:

- Prevention or detection of crime
- The apprehension or prosecution of offenders
- Assessment or collection of tax, duty or imposition of a similar nature.

The school will treat requests for information from an official bodies related to criminal or taxation purposes under Data Protection Act 2018 – schedule 2, part 1, paragraph 2 and GDPR Article 6 (1) (d). The school requires the requestor to complete the Request for personal data form.

Generally, the school reserves the right not to release the data but there may be situations such as the receipt of a court order that requires the school to release the information.

Access to Pupils' Records

There are two distinct rights to information held by schools about pupils.

1. Subject Access Right – under GDPR a pupil has the right to a copy of their information; this type of request is a Subject Access Request (SAR). In certain circumstances requests may be made by a parent on behalf of the child.

2. Rights to the educational record – under the Education (Pupil Information) (England) Regulations 2005, a parent has the right to access their child's educational record.

Subject Access Requests – a child or young person will always be the owner of their personal information as defined within the GDPR. However, if a young person is incapable of making their own decisions, which needs to be assessed on a case by case basis, but is generally accepted as being under the age of 12 years, the primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the best interests of the child or young person.

The school will respond to the request within 1 calendar month of receipt; this may be extended by up to 2 further calendar months if a request is complex, in which case the school will contact the requester within 1 calendar month of receipt and explain why the extension is necessary.

Education (Pupil Information) (England) Regulations 2005 – requests from parents to view their child's educational record will be dealt with by the Board of Governors. The request must be made in writing and a response must be provided within 15 school days.

The pupil cannot prevent a parent from accessing their educational record under the Pupil Information Regulations, but they can object to their parent accessing information through a Subject Access Request, assuming that the child in question is sufficiently mature to make such a decision.

The Protection of Freedoms Act 2012

The Protection of Freedoms Act was introduced in February 2011 and came into force on 9th May 2012 with the commencement orders coming into force in July 2012. It is an Act to impose consent and other requirements in relation to processing of biometric information relating to children, to provide a code of practice about surveillance camera systems amongst other things.

CCTV AND OTHER SURVEILLANCE CAMERA TECHNOLOGY

CCTV surveillance has become a common feature of our daily lives and now there is an increasing use of these in and around educational settings. Information held by the school is covered under GDPR; capture of CCTV must be in line with relevant codes of practice including the Surveillance Camera Code of Practice issued by the Surveillance Camera Commissioner, available here: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice and the CCTV Code of Practice issued by the Information Commissioner's Office, available here:https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Recorded material will be stored in a way that maintains the integrity of the image. Once there is no reason to retain the recorded images, **they will be deleted**.

In area where CCTV surveillance is being carried out there will be clear markings to reflect this.

Subject access requests for CCTV images

Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This will be provided within 1 calendar month of receiving a request.

BIOMETRIC DATA

Biometric technologies are those which automatically measure people's physiological or behavioural characteristics. Examples include automatic fingerprint identification, iris and retina scanning, face recognition and hand geometry, and their use is becoming increasingly popular in educational settings.

Under GDPR Biometric Data which is used to identify an individual (e.g. finger-prints, iris recognition) is classed as special category data and as such the school must satisfy a special category condition in addition to the legal basis when processing the data.

A Data Protection Impact Assessment should be carried out to ensure that the special category condition is met and that all risks are identified and mitigated.

Before the first processing of a child's biometric information, the school will notify each parent of the child:

- Of its intention to process the child's biometric information
- That the parent may object at any time to the processing of the information.

Schools must comply with data protection principles and additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012 in order to use Biometric Technologies. The school needs to ensure that:

a) each parent of a child is notified of the school's intention to use the child's biometric data
b) written consent of at least one parent must be obtained before the data are taken from the child
c) **In no circumstances can a child's biometric data be processed without written consent.**

The school is not required to notify a parent, or obtain the consent of a parent, if the school is satisfied:

a) The parent cannot be found
b) The parent lacks capacity (within the meaning of the Mental Capacity Act 2005) to object or consent (as the case may be) to the processing of the child's biometric information
c) The welfare of the child requires that the parents is not contacted
d) It is otherwise not reasonable practicable to notify the parent or (as the case may be) obtain the consent of the parent.

Disclosure of non - personal information / FOI Requests

The school as a public authority is subject to The Freedom of Information Act 2000 and all requests for information that is not personal information must be treated as a Freedom of Information request. FOI requests must be fully responded within 20 (school) working days by law. The information will be provided unless the school can provide an exemption under the FOI act

A more detailed guide to FOI exemptions is here:
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

https://ico.org.uk/media/for-organisations/documents/1643/foi_hints_for_practitioners_handing_foi_and_eir_requests_2008.pdf

Roles and Responsibilities

The Senior Information Risk Owner (SIRO) for the school is the Headteacher.
They are responsible for:

- Owning and updating this policy
- Owning the information risk register
- Appointing Information Asset Owners (IAOs) for each Information Asset
- Advocating information risk management and raising awareness of information security issues
- After liaising with the Data Protection Officer, determining whether a security incident is of sufficient severity to report to the Information Commissioner's Office, and if the risk of adverse impact on the data subject(s) is such that they should be notified

The Data Protection Officer for the school is appointed through an external adviser by the cluster group of schools. They are responsible for:

- Informing and advising on the school's obligations to comply with GDPR and other data protection laws
- Monitoring compliance with GDPR and other data protection laws
- Monitoring compliance with the school's data protection policies and procedures, including managing internal data protection activities, raising awareness of data protection issues, training staff and conducing internal audits
- Advising on and monitoring Data Protection Impact Assessments
- Acting as first point of contact for individuals whose data is process (pupils, parents, employees etc) and for the Information Commissioner's Office, and any other relevant supervisory authorities

Information Asset Owners are responsible for:

- Ensuring the information is used for the purpose it was collected
- How information has been amended or added to over time
- Who has access to protected data and why

All staff are responsible for ensuring that information is managed according to this policy.

Signed on behalf of the Governing body:

Signed _____ Date _____

Chair of the Governing body

Appendix 1

Processing Personal Data: Legal Basis, Special Category Data and Special Category Conditions

Legal Basis: The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Special Category Data: GDPR identifies that some information is particularly sensitive and therefore needs extra protection:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership Health
- Sexual life or orientation
- Genetic data (e.g. blood samples DNA)
- Biometric data to identify an individual (e.g. finger-prints, iris recognition)
- Financial information

Special Category Conditions: Under GDPR if you are processing special category data you need to meet a special category condition in addition to the legal basis identified above. The special category conditions are:

- The data subject has given explicit consent
- Necessary to protect the vital interests where the data subject is physically or legally incapable of giving consent

- The data has been made publically available by the data subject
- Necessary for the purposes of preventative or occupational medicine, for example the assessment of the working capacity of an employee
- Required for exercising rights in the field of employment and social security or social protection
- Processing is carried out by a foundation or not-for-profit body in the course of its legitimate activities
- Necessary to process legal claims
- Necessary for archiving statistical or historical research which is in the public interest
- Necessary for reasons of substantial public interest on the basis of UK law which shall be proportionate to the aim pursued

Data relating to criminal convictions or offences: Under GDPR information relating to criminal convictions **(**includes all DBS checks even if they show no convictions/offences) can only be processed process if you are doing so in an official capacity or have specific legal authorisation to do so.

(Please note that Section 3 of the Data Protection Bill sets out specific data protection principles to be considered when processing personal data for law enforcement purposes. This section of the policy will therefore be refreshed at such time as the Bill is passed and becomes UK law)

Appendix 2

Retention schedules and impact levels

NOTE TO SCHOOLS:

This retention schedule is based on guidance from the records management society:
https://cdn.ymaws.com/irms.org.uk/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

It encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

Please also note that for a number of years an Independent Inquiry into Child Sexual Abuse (formally the Goddard Inquiry) has been running. For the life of this Inquiry we must not destroy records that are:

- **connected with child protection**
- **connected with child sexual abuse**
- **related to individuals working with children**

In terms of how this fits with GDPR requirements, the suspension of the disposal of these records is covered by the Inquiries Act 2005 which makes it a criminal offence for anyone to knowingly destroy, alter or conceal records and information which is or may be relevant to the Inquiry In effect this "top trumps" GDPR. A letter was posted on Exranet about this

https://extranet.bolton.gov.uk/website/pages/view.aspx?f=Retention and Destruction of Records May 2018-HR.pdf

1 Child Protection

These retention periods should be used in conjunction with the document “Safeguarding Children and Safer Recruitment in Education which can be downloaded from this link:

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record		Protective Marking Classification
1.1	Child Protection	Yes	Education Act 2002, s175, related guidance “Safeguarding Children in Education”, September 2004	DOB + 25 years[1]	SECURE DISPOSAL	Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example)	**IL4-Confidential**

1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance)	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL	The following is an extract from “Safeguarding Children and Safer Recruitment in Education” p60	**L4-Confidential**
			Education Act 2002 guidance “Dealing with Allegations of Abuse against Teachers and Other Staff” November 2005			Record Keeping	

						5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future DBS Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."	

[1] This amendment has been made in consultation with the Safeguarding Children Group

2 Governors							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
2.1	Minutes						
	Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives	**IL3 - RESTRICTED**
	Inspection copies	No		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they should be SECURELY DISPOSED		**IL3 - RESTRICTED**
2.2	Agendas	No		Date of meeting	SECURE DISPOSAL		**IL1–Unclassified**
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**

2.4	Annual Parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
2.5	Instruments of Government	No		Permanent	Retain in school whilst school is open	Transfer to Archives when the school has closed	**IL1–Unclassified**
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required	Transfer to Archives	**IL1–Unclassified**
2.7	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL	It may be appropriate to offer to the Archives for a sample to be taken if the school has been through a difficult period	**IL1–Unclassified**
2.8	Statutory Policy documents (does not include school specific policies such as writing policies etc.)	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes SECURE DISPOSAL		**IL3 - RESTRICTED**

2.10	Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL2–PROTECT**
3 Management							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
3.1	Log Books	Yes[1]		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives	**IL3 - RESTRICTED**
3.2	Minutes of the Senior Management Team and other internal administrative bodies	Yes[1]		Date of meeting + 5 years	Retain in the school for 5 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL3 - RESTRICTED**
3.3	Reports made by the head teacher or the management team	Yes[1]		Date of report + 3 years	Retain in the school for 3 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL3 - RESTRICTED**

3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
3.6	Professional development plans (Management plans for professional development plans of staff)	Yes		Closure + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.7	School development plans	No		Closure + 6 years	Review	Offer to the Archives	**IL2–PROTECT**
3.8	Admissions – if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.9	Admissions – if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**

3.10	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.11	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**

[1] From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998.

3 Management

	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
4.1	Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives	**IL3 - RESTRICTED**
4.2	Attendance registers	Yes	The Education (Pupil Registration) (England) Regulations 2006 (No. 1751)	Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]		**IL3 - RESTRICTED**

4.3	Pupil record cards						
4.3a	*Primary*	Yes		Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service		**IL3 - RESTRICTED**
4.3b	*Secondary*	Yes	Limitation Act 1980	DOB of the pupil + 25 years[1]	SECURE DISPOSAL		**IL3 - RESTRICTED**
4.4	Pupil files						
4.4a	*Primary*	Yes		Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service		**IL3 - RESTRICTED**
4.4b	*Secondary*	Yes	Limitation Act 1980	DOB of the pupil + 25 years[2]	SECURE DISPOSAL		**IL3 - RESTRICTED**
4.5	Special Educational Needs files, reviews and Individual	Yes		DOB of the pupil + 25 years the review	SECURE DISPOSAL		**IL4-Confidential**

	Education Plans			NOTE: This period is the minimum that any pupil file should be kept. Some choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. The element of business risk is an analysis involved in any decision to keep the records longer than the minimum retention period.			
4.6	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
4.7	Absence books	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
4.8	Examination results	Yes					
4.8a	*Public*	No		Year of examinations + 6 years	SECURE DISPOSAL	Any certificates left unclaimed should be returned to the appropriate Examination Board	**IL2–PROTECT**
4.8b	*Internal examination results*	Yes		Current year + 5 years[3]	SECURE DISPOSAL		**IL2–PROTECT**

4.9	Any other records created in the course of contact with pupils	Yes/ No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL		**IL3 - RESTRICTED**
4.10	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**
4.11	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**
4.12	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**
4.13	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending		**IL3 - RESTRICTED**
4.14	Children's SEN Files	Yes		DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**
4.15	Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL		**IL3 - RESTRICTED**

4.16	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL		**IL3 - RESTRICTED**
4.17	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 14 years[4]	N	SECURE DISPOSAL or delete securely	**IL2–PROTECT**
4.18	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years[7]	N	SECURE DISPOSAL or delete securely	**IL2–PROTECT**
4.19	Walking Bus registers	Yes		Date of register + 3 years 	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]		**IL3 - RESTRICTED**

				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			

[1] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service

[2] As above

[3] If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

[4] This retention period has been set in agreement with the Safeguarding Children's Officer

5 Curriculum

	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record		Protective Marking Classification
5.1	Curriculum development	No		Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL		**IL1–Unclassified**

5.3	School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL1–Unclassified**
5.4	Schemes of work	No		Current year + 1 year This retention period starts once the document has been superseded	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL1–Unclassified**
5.5	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL1–Unclassified**
5.6	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**

5.7	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**
5.8	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**
5.9	Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**
5.1	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.11	SATS records	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.12	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.13	Value added records	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.14	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**

6 Personnel Records held in Schools							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
6.2	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL		**IL2–PROTECT**
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL		**IL2–PROTECT**
6.4	Pre-employment vetting information (including DBS Checks)	No	DBS Guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]		**IL2–PROTECT**
6.41	Single Central Record	Yes	ISA guidelines	Keep until school closure	Offer to local authority designated officer		**IL2–PROTECT**
6.5	Disciplinary proceedings:		**Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.**				
6.5a	*oral warning*	Yes		Date of warning + 6 months.	SECURE DISPOSAL		**IL2–PROTECT**
6.5b	*written warning – level one*	Yes		Date of warning + 12 months.	SECURE DISPOSAL		**IL2–PROTECT**

6.5c	*final warning*	Yes		Date of warning + 12 months.	SECURE DISPOSAL		**IL2–PROTECT**
6.5d	*case not found*	Yes		If child protection related please see 1.2	SECURE DISPOSAL		**IL2–PROTECT**
6.6	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		**IL2–PROTECT**
6.7	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL		**IL2–PROTECT**
6.8	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL		**IL2–PROTECT**
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SECURE DISPOSAL		**IL2–PROTECT**

6.1	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
6.11	Proof 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.		**IL2–PROTECT**

[1] If this is placed on a personal file it must be weeded from the file.

7 Health and Safety

	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
7.1	Accessibility Plans	No	Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980				

7.2a	*Adults (All Accidents)*	Yes		Date of incident + 7 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
7.2b	*Children (All Accidents)*	Yes		DOB of child + 25 years[1]	SECURE DISPOSAL		**IL3 - RESTRICTED**
7.3	COSHH	No		Current year + 10 years [where appropriate an additional retention period may be allocated]	SECURE DISPOSAL		**IL1–Unclassified**
7.4	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
7.5	Policy Statements	No		Date of expiry + 1 year	SECURE DISPOSAL		**IL1–Unclassified**
7.6	Risk Assessments	No		Current year + 3 years	SECURE DISPOSAL		**IL1–Unclassified**
7.7	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		**IL1–Unclassified**
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	No		SECURE DISPOSAL			**IL1–Unclassified**
7.9	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**

[1] A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.

8 Administrative

	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record		Protective Marking Classification
8.1	Employer's Liability certificate	No		Closure of the school + 40 years	SECURE DISPOSAL		**IL1–Unclassified**
8.2	Inventories of equipment and furniture	No		Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**
8.3	General administrative records (records not specifically listed elsewhere)	No		Current year + 5 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
8.4	School brochure or prospectus	No		Current year + 3 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
8.5	Circulars (staff/parents/pupils)	No		Current year + 1 year	SECURE DISPOSAL		**IL1–Unclassified**
8.6	Newsletters, Ephemera	No		Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives	**IL1–Unclassified**

						[The appropriate archivist will then take a sample for permanent preservation]	
8.7	Visitors book	No		Current year + 2 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
8.8	PTA/Old Pupils Associations	No		Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
9 Finance							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
9.1	Annual Accounts	No	Financial Regulations	Current year + 6 years		Offer to the Archives	**IL2–PROTECT**
9.2	Loans and grants	No	Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL2–PROTECT**
9.3	Contracts						
9.3a	under seal	No		Contract completion date + 12 years	SECURE DISPOSAL		**IL2–PROTECT**
9.3b	under signature	No		Contract completion date + 6 years	SECURE DISPOSAL		**IL2–PROTECT**

9.3c	monitoring records (Bolton MBC Corporate Property Unit may hold these records on the schools behalf)	No		Current year + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
9.4	Copy orders	No		Current year + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
9.5	Budget reports, budget monitoring etc	No		Current year + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
9.6	Invoice, receipts and other records covered by the Financial Regulations	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.7	Annual Budget and background papers	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.8	Order books and requisitions	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.9	Delivery Documentation	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.1	Debtors' Records	No	Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.11	School Fund – Cheque books	No		Current year + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
9.12	School Fund – Paying in books	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.13	School Fund – Ledger	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**

9.14	School Fund – Invoices	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.15	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.16	School Fund – Bank statements	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.17	School Fund – School Journey books	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.18	Student Grant Applications	Yes		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.19	Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
9.20	Petty cash books	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
10 Property							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
10.1	Title Deeds	No		Permanent	Permanent these should follow the property unless the property has been registered at the Land Registry	Offer to Archives if the deeds are no longer needed	**IL2–PROTECT**
10.2	Plans	No		Permanent	Retain in school whilst operational	Offer to Archives[1]	**IL3 - RESTRICTED**
10.3	Maintenance and contractors	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
10.4	Leases	No		Expiry of lease + 6 years	SECURE DISPOSAL		**IL2–PROTECT**

10.5	Lettings	No		Current year + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
10.6	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
10.7	Maintenance log books	No		Last entry + 10 years	SECURE DISPOSAL		**IL1–Unclassified**
10.8	Contractors' Reports	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**

[1] If the property has been sold for private housing then the archives service will embargo these records for an appropriate period of time to prevent them being used to plan or carry out a crime.

11 Local Education Authority

	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
11.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**
11.3	Circulars from LEA	No		Whilst required operationally	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**

12 Department for Children, Schools and Families

	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
12.1	OFSTED reports and papers	No		Replace former report with any new inspection report	Schools may wish to retain copies of former reports for longer	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL2–PROTECT**

12.2	Returns	No		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
12.3	Circulars from Department for Children, Schools and Families	No		Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
13 Connexions							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
13.1	Service level agreements	No		Until superseded	SECURE DISPOSAL		**IL1–Unclassified**
13.2	Work Experience agreement	Yes		DOB of child + 18 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
14 Schools Meals							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
14.1	Dinner Register	Yes		C + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
14.2	School Meals Summary Sheets	Yes		C + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
15 Family Liaison Officers and Parent Support Assistants							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
15.1	Day Books	Yes		Current year + 2 years then review	SECURE DISPOSAL		**IL3 - RESTRICTED**

15.2	Reports for outside agencies – where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL		**IL3 - RESTRICTED**
15.3	Referral forms	Yes		While the referral is current then	SECURE DISPOSAL		**IL4-Confidential**
15.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL		**IL2–PROTECT**
15.5	Contact database entries (FLO contact records with agencies and family member)	Yes		Current year then review, if contact is no longer active then destroy	DELETE		**IL2–PROTECT**
15.6	Group Registers (FLO work)	Yes		Current year + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
15.7	Early Help Assessments	Yes		Current year + 6	SECURE DISPOSAL		**IL4-Confidential**
16 Early Years Provision (Childcare / Nursery provision etc.)							
16.1 Records to be kept by Registered Persons - All Cases							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
16.1.1	The name, home address and date	Yes		Closure of setting + 50 years			**IL3 - RESTRICTED**

	of birth of each child who is looked after on the premises			[These could be required to show whether or not an individual child attended the setting in a child protection investigation]			
16.1.2	The name, home address and telephone number of a parent of each child who is looked after on the premises	Yes		If this information is kept in the same book or on the same form as in 16.1.1 then the same retention period should be used as in 16.1.1			**IL3 - RESTRICTED**
				If the information is stored separately, then destroy once the child has left the setting (unless the information is collected for anything other than emergency contact)			
16.1.3	The name, address and telephone number of any person who will be looking after children on the premises	Yes		See 16.4.5 below			**IL3 - RESTRICTED**

16.1.4	A daily record of the names of children looked after on the premises, their hours of attendance and the names of the persons who looked after them	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003	The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). If these records are likely to be needed in a child protection setting (see 16.1.1 above) then the records should be retained for closure of setting + 50 years			**IL3 - RESTRICTED**
16.1.5	A record of accidents occurring on the premises and incident books relating to other incidents	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003[1]	DOB of the child involved in the accident or the incident + 25 years			**IL2–PROTECT**
				If an adult is injured then the accident book must be kept for 7 years from the date of the incident			

16.1.6	A record of any medicinal product administered to any child on the premises, including the date and circumstances of its administration, by whom it was administered, including medicinal products which the child is permitted to administer to himself, together with a record of parent's consent	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003[2]	DOB of the child being given/taking the medicine + 25 years			**IL3 - RESTRICTED**
16.1.7	Records of transfer	Yes		One copy is to be given to the parents, one copy transferred to the Primary School where the child is going			**IL2–PROTECT**
16.1.8	Portfolio of work, observations and so on	Yes		To be sent home with the child			**IL2–PROTECT**

16.1.9	Birth certificates	Yes		Once the setting has had sight of the birth certificate and recorded the necessary information the original can be returned to the parents. There is no requirement to keep a copy of the birth certificate.			**IL3 - RESTRICTED**

[1] The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). The Statute of Limitations states that a minor may make a claim for 7 years from their eighteenth birthday, therefore the retention should be for the longer period.

[2] The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). The NHS records retention schedule states that any records relating to a child under the age of 18 should be retained until that child reaches the age of 25 years. Therefore, the retention should be DOB of the child being given/taking the medicine + 25 years

16.2 Records to be kept by Registered Persons - Day Care (Relates to nursery and child minding provision

	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
16.2.1	The name and address and telephone number of the registered person and every other person living or employed on the premises	Yes		See 16.4 below			**IL3 - RESTRICTED**
16.2.2	A statement of the procedure to be followed in the event of a fire or accident	No		Procedure superseded + 7 years			**IL1–Unclassified**

16.2.3	A statement of the procedure to be followed in the event of a child being lost or not collected	No		Procedure superseded + 7 years			**IL1–Unclassified**
16.2.4	A statement of the procedure to be followed where a parent has a complaint about the service being provided by the registered person	No		Until superseded			**IL1–Unclassified**
16.2.4	A statement of the arrangements in place for the protection of children, including arrangements to safeguard the children from abuse or neglect and procedures to be followed in the event of allegations of abuse or neglect	Yes		Closure of setting + 50 years			**IL4-Confidential**
				[These could be required to show whether or not an individual child attended the setting in a child protection investigation]			
16.3 Records to be kept by Registered Persons - Overnight provision – under 2's							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**	

16.3.1	Emergency contact details for appropriate adult to collect the child if necessary	Yes		Destroy once the child has left the setting (unless the information is collected for anything other than emergency contact)			**IL3 - RESTRICTED**
16.3.2	Contract, signed by the parent, stating all the relevant details regarding the child and their care, including the name of the emergency contact and confirmation of their agreement to collect the child during the night	Yes		Date of birth of the child who is the subject of the contract + 25 years			**IL3 - RESTRICTED**
16.4 Other Records – Administration							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
Financial Records							
16.4.1	Financial records – accounts, statements, invoices, petty cash etc	No		Current year + 6 years			**IL2–PROTECT**
Insurance							
16.4.2	Insurance policies – Employers	No	Employers Liability	The policies are kept for a			**IL1–Unclassified**

	Liability		Financial Regulations	minimum of 6 years and a maximum of 40 years depending on the type of policy			
16.4.3	Claims made against insurance policies – damage to property	Yes		Case concluded + 3 years			**IL2–PROTECT**
16.4.4	Claims made against insurance policies – personal injury	Yes		Case concluded + 6 years			**IL2–PROTECT**
Human Resources							
16.4.5	Personal Files - records relating to an individual's employment history	Yes		Termination + 6 years then review			**IL3 - RESTRICTED**
16.4.6	Pre-employment vetting information (including DBS checks)	No	DBS guidelines	Date of check + 6 months			**IL4-Confidential**
16.4.7	Staff training records – general	Yes		Current year + 2 years			**IL2–PROTECT**
16.4.8	Training (proof of completion such as certificates, awards, exam results)	Yes		Last action + 7 years			**IL2–PROTECT**
	Premises and Health and Safety						
16.4.9	Premises files (relating to maintenance)	No		Cessation of use of building + 7 years then review			**IL1–Unclassified**

16.4.10	Risk Assessments	No		Current year + 3 years			**IL1–Unclassified**

[1] For Data Protection purposes the following information should be kept on the file for the following periods :

• all documentation on the personal file	Duration of employment
• pre-employment and vetting information	Start date + 6 months
• records relating to accident or injury at work	Minimum of 12 years
• annual appraisal/assessment records	Minimum of 5 years
• records relating to disciplinary matters (kept on personal files)	
o oral warning	6 months
o first level warning	6 months
o second level warning	12 months
o final warning	18 months

Appendix 3

Information Security Incident Report Form

All boxes must be completed

School Logo

To be completed by the person reporting the breach

Name	
Job title	
Department / Section (if applicable)	
Telephone number	
E-mail address	
Date	

What has happened? Please provide as much information as you can about what has happened, what went wrong and how; include a description of the data, eg: format, volume, from which system, and the location of the breach.
How did you find out about the breach? If you were not the person who originally found there had been a breach, please explain how you found out about it <u>and</u> how they found out about it.
Was the breach caused by a cyber incident?

Yes		**No**		**Not yet known**	

When was the breach discovered?	**Date:**		**Time:**	
When did the breach occur?	**Date:**		**Time:**	

What has happened to the information? (Please select all that apply)					
Destroyed		**Lost**		**Stolen**	
Altered		**Unauthorised Disclosure**		**Unauthorised Access**	
Other (please give details below)					

Categories of personal data included in the breach (Please select all that apply)			
Basic personal identifiers (eg: name, contact details)		**Identification data (eg: usernames, passwords)**	
Racial or ethnic origin		**Political opinions**	
Religious or philosophical beliefs		**Trade union membership**	
Health		**Sexual life or orientation**	
Gender reassignment data		**Genetic or biometric data**	
Financial information		**Criminal convictions or offences**	
Official documents (eg: driving licences)		**Location data**	
Other (please give details below)		**Not yet known**	

How may data subjects could be affected?	

Categories of data subjects affected (Please select all that apply)			
Employees		**Pupils**	
Parents / Carers		**Governors**	
Volunteers		**Other (please give details below)**	

What is the possible impact of the breach on the data subjects?					
Has there been any actual harm to data subjects? (If yes, please give details below)					
Yes		**No**		**Not yet known**	
What is the likelihood that data subjects will experience significant consequences as a result of the breach? (Please select one option and give further details below)					
Very likely		**Likely**		**Neutral**	
Unlikely		**Very unlikely**		**Not yet known**	
Have you told the data subjects about the breach?					
Yes		**About to or in process of telling them**			
No, but they're already aware		**No, but planning to tell them**			
No, decided not to tell them		**Not yet decided whether to tell them**			
Seeking advice from DPO		**Other (Please give details below)**			
Have you told, or are you planning to tell, any other organisations (e.g. police, regulatory body) about the breach? (If yes, please give details below. If you have a crime reference number, please include it)					
Yes		**No**			
Seeking advice from DPO		**Other (Please give details below)**			

What measures have been taken to deal with the breach? (e.g. contacting the person sent in formation in error, auto-erased lost laptop)
Has the data been recovered? (Please give details - if the breach is due to a misdirected email, include whether you have had confirmation that the recipient has deleted it and whether it was read or unread)

Yes		**No**		**Partially**	

What measures have been taken / are proposed to mitigate further breaches?
If there is any further information you think should be considered please include it here.

To be completed by the Data Protection Officer

Form received by DPO	**Date:**		**Time:**			
Was the form received within 24 hours of the breach being discovered?			**Yes**		**No**	
If no, was a reason given? (Please give details below)			**Yes**		**No**	
Is the information on the form complete?			**Yes**		**No**	
If not, what further information is required? (Please give details below)						

Breach reported to SIRO	**Yes**		**No**		**Date**	
Breach reported to Head Teacher	**Yes**		**No**		**Date**	
Breach reported to Chair of Governors	**Yes**		**No**		**Date**	

What measures have been agreed should be taken to deal with the breach?
What measures have been agreed should be taken to mitigate harm caused by the breach?
Have data subjects been told about the about the breach (if not already done by person reporting it)?

Yes		**About to or in process of telling them**	
No, but they're already aware		**No, but planning to tell them**	
No, decided not to tell them		**Other (Please give details below)**	

Does the breach warrant a report to the ICO?	**Yes**		**No**	
If yes, when was the breach reported to the ICO?	**Date:**		**Time:**	
Was report to ICO made within 72 hours?	**Yes**		**No**	

If report was not made within 72 hours, please provide justification for late reporting below.

What has been identified as the root cause(s) of the breach following investigation?

What corrective actions have been identified following investigation?

Action	Target Date	Owner	Date Completed

DPO Sign-off		**Date**	
Head Teacher Sign-off		**Date**	
Date Incident Investigation Closed			