Frogwell Primary School (2017 – 2019)
Data Protection Policy

1. Rationale:

As a school we collect and handle increasing amounts of personal information and have a statutory requirement to comply with The Data Protection Act 1998("DPA") and the GDPR regulations from May 2018. The reason we collect and handle data is to enable us to:

- *Keep children safe by knowing who they are, what needs they have, where they live and who to contact in the case of an emergency or any other school-related reason.*
- *Recording and tracking pupil attainment and progress information so that we can plan to meet the social, emotional, behaviour and learning needs of the child.*
- *Ensure the safety and well-being of staff.*
- *To fulfil contractual obligations such as PAYE and performance appraisal.*

Schools should have clear policies and procedures for dealing with personal information, and be registered with the Information Commissioner's Office ("ICO"). Schools should have systems in place to reduce the chances of a loss of personal information, otherwise known as a data breach which could occur as a result of theft, loss, accidental disclosure, equipment failure or hacking.

2. Aims and Objectives:

At Frogwell Primary School we build our aims around the school's core values of equipping every pupil with the skills to become a lifelong learner and caring and considerate member of their community. We also draw on aspects of the values promoted through the International Primary Curriculum which have underpinned the way we have promoted pupils approaches to learning and lifelong learning. These values are interpreted within the aims of our Data Protection Policy in the following ways:

Morality	• To foster an ethos of trust within the school where all who handle personal data do so within the framework of the law. • To ensure that confidentiality is a whole school issue and that in lessons ground rules are set for the protection of all. • To ensure that if there are child protection issues then the correct procedure is followed as outlined in the school's Child Protection policy.
Communication	• To ensure that staff, parents and pupils are aware of the school's Data Protection Policy and procedures and how personal data should be processed, stored, archived and deleted/destroyed • To provide consistent messages in school about handling information about children, staff and families once it has been received. • To ensure that children/parents know that school staff cannot offer unconditional confidentiality.
Cooperation	• To reassure children that their best interest will be maintained. • To ensure that staff and parents have a right of access to all records held on them or their child(ren), except where the sharing of these could endanger the child.
Respect	• To protect personal data at all times and to give all school staff clear, unambiguous guidance as to their legal and professional roles and to ensure good practice throughout the school which is understood by children, parents / carers and staff. • To ensure that there is equality of provision and access for all including rigorous monitoring of cultural, gender and special educational needs.

3. Data Protection Principles

The Data Protection Act 1998 (DPA) and the General Data Protection Regulations (GDPR) establish and recognise eight principles that must be adhered to by the school at all times. These are that:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

4. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In the Frogwell Primary School environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar approach takes place with managing school data. The DPA defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a " Potential Data Breach" which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

4.1 Personal data

Frogwell Primary School has access to a wide range of personal information and data. This data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.
This includes:-

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, disciplinary records.
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

4.2 Sensitive Personal data

Sensitive personal data is defined as information that relates to the following eight categories: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and criminal offences, criminal proceedings.
It requires a greater degree of protection and in Frogwell Primary School will include:-

- Staff Trade Union details
- Information on the racial or ethnic origin of a child or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff
- Information relating to any criminal offence of a child, family member or member of staff.

Note *– On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely, for instance in the staff room.*

4.3 Other types of Data not covered by the Data Protection act or GDPR.

This is data that does not identify a living individual and therefore is not covered by the remit of the DPA this may fall under other access to information procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publically (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (If the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provide additional information on their website See
http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

5 Responsibilities

The Headteacher and Governing Body are responsible for Data Protection. They will establish two key roles within the school to manage data. The first of these positions is the Data Protection Officer (DPO) and the second position is the Data Protection Controller (DPC). These two post holders will ensure that the school manages data within the law and responds appropriately if there are any data breeches.

5.2 Risk Management – Roles

The DPO's minimum tasks are defined in Article 39 of the GDPR and their responsibilities include, but are not limited to:

- Educating the school and its staff on important compliance requirements
- Training staff involved in data processing.
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the school and GDPR Supervisory Authorities.
- Monitoring performance and providing advice on the impact of data protection efforts.
- Maintaining comprehensive records of all data processing activities.
- Interconnecting with data subjects or parents to inform them about: how their data is being used; their rights to have their, or their child's personal data erased; the measures in place to protect their, or their child's, personal information.

Within the above role the DPO also:
DPO has to work with the DPC within the school. He / she has to be independent of any data input within that organisation. The DPO could be the head or DPC of another school working with another school.

In Frogwell Primary School we work in partnership with another school to achieve a DPO who has an understanding of data protection from an educational perspective but who can be objective and impartial in relation to our school's organisation around data protection.

The appointed person in this case is Sheridan Upton who is the DPC for St Paul's Primary School. Conversely our DPC acts as DPO in their school.
The DPO has a responsibility to report to the ICO. If they do not do this they are legally accountable. Any matters in relation to Data Protection to be email to dataprotection@frogwell.wilts.sch.uk.

The DPC is involved with the ongoing day to day operations within the school. Their responsibilities include, but are not limited to ensuring that the school is compliant with the following rules:

- That personal data is processed legally and fairly
- The data the school collects is collected for legitimate purposes and used accordingly
- The data collected by the school is adequate and relevant and is not excessive in relation to the reason it has been collected (or processed)
- Data collected by the school is updated regularly and is accurate
- That any personal data held by the school is rectified, removed and is blocked if incorrect
- Anything that identifies individuals must not be kept too long
- Anything personal must be protected against accidental, unlawful destruction, alteration and disclosure; especially when it involves processing data over networks

Data controllers must implement appropriate security measures and these measures need to have the appropriate level of protection for the data stored and processed.
If an individual (staff member, parent, student) believes that their data has been compromised they can send a complaint to the 'data controller', if they feel that the schools handling of their complaint is not to their satisfaction they can then file a complaint with the national supervisory data protection authority.
Within the above role the DPC also:

- Keeps a log of data breeches and talks to staff member breeching so that they can put things right.
- Reviews the log on a regular basis. Their responsibility is to identify if it is a conduct or capability action if things do not change. If this becomes serious it is reported to the DPO and evidence is then prepared to submit to the ICO
- The DPC needs to meet with the DPO on a regular basis (quite possibly monthly).

Under GDPR data controllers and data processors will have equal liability should there be a data breach.

5.3 Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

6 Legal Requirements

6.2 Registration

The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration): http://ico.org.uk/for_organisations/data_protection/registration

6.3 Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through a letter.

See Appendix 2 for the school's current Privacy Notices.

7 Transporting, Storing and Deleting personal Data

- The policy and processes of the school will comply with the guidance issued by the ICO here

7.2 Information security - Storage and Access to Data

7.2.1 Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.
- The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

7.2.2 Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

7.2.3 Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

7.2.4 Photographs and Images

- Images of pupils will only be processed and transported by use of encrypted devices and permission for this will be obtained in the privacy agreement.
- Images will be protected and stored in a secure area.

7.2.5 CCTV

- Capturing and/or recording images of identifiable individuals is processing personal information and is done in line with the data protection principles. As a school we only collect personal information in the form of CCTV images to help protect school assets and in some areas such as the playground to support the maintenance of good order in the school. Cameras are only sited at strategic access points and in areas where the school can gain a wide view of an area (ie;. the school playground or carpark).
- The length of time recordings are kept and how we dispose of them is detailed in the school's Information Retention Policy and the need to review any footage. As a general

rule the only people who will view images are members of the school leadership team or persons directed by them or members of the police where the school is investigating crime against persons on the premises or the school as a physical space.
- The subjects of CCTV images have the right to access their images in line with the school's retention and accessing policies.

7.2.6 Cloud Based Storage

- The school / academy has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

7.3 Third Party data transfers

- As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

7.4 Retention of Data

- The school will keep some forms of information for longer than others. Information will not be kept indefinitely, unless there are specific requirements. In line with principle 5 of the data protection act information should not be kept longer than is necessary. Appendix 3 gives a breakdown of timescales for the retention of various types of information.
- When data is no longer required it will be appropriately destroyed. Appendix 3 outlines the procedure to be used for the disposal of information.
- Personal data that is no longer required will be destroyed and this process will be recorded.

7.5 Systems to protect data

7.5.1 Paper Based Systems

- All paper based OFFICIAL or OFFICIAL – SENSITIVE (or higher) material must be held in lockable storage, whether on or off site.
- Paper based personal information sent to parents will be checked by a member of the senior management team before the envelope is sealed.

7.5.2 School Websites

- Uploads to the school website will be checked prior to publication ensure that personal data will not be accidently disclosed and that images uploaded only show pupils where prior permission has been obtained

7.5.3 E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- E-mails containing sensitive information should be encrypted, for example by attaching the sensitive information as a password protected word document. The recipient will then need to contact the school for access to a one-off password

7.6 Disposing of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required as specified in the IRMS Information Management Toolkit for Schools The disposal of personal data, in either paper or electronic form, will be conducted in a way that makes reconstruction highly unlikely. Electronic files will be securely overwritten, in accordance with government guidance (see earlier section for reference to the Cabinet Office guidance), and other media will be shredded, incinerated or otherwise disintegrated for data. A Destruction Log is kept of all data that is disposed of. The log includes the document ID / Documents ID, classification, date of destruction, method of destruction and authorisation for destruction.
As outlined above (7.4) Appendix 3 details the school's retention and destruction schedule for school data. This will be reviewed in light of any changes stipulated in statutory guidance. The information detailed in Appendix 3 is drawn from the IRMS Information Management Toolkit for Schools document (February 2016)

8. Subject Access Requests

- Parents / carers of all pupils / students and staff have the right to obtain confirmation from the school as to whether or not personal data concerning a child or them personally is being processed, and, where this is the case, access to this personal data and information.
- The school will provide a copy of the personal data and may charge a reasonable fee for additional copies that is based on the administrative costs to do this. Where the request is by electronic means, and unless otherwise requested by the subject, the information will be provided in a commonly used electronic form.
- The right to obtain a copy of personal information will be completed within one month. This is to allow the school to process the request without adversely affecting the rights and freedoms of others.
- The school does however have the right to refuse or charge for requests that are manifestly unfounded or excessive. Where the school exercises this right the school will inform the subject of their right to complain to the supervisory authority.

9. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach the DPC will inform the head teacher and DPO
- The school will follow the procedures set out in its Data Breach Policy.

In addition to this audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example. The school's policy for reporting, managing and recovering from information risk incidents establishes and details the:

- "Responsible person" for each incident;
- Communication plan, including escalation procedures;
- Results of the plan of action for rapid resolution; and
- Plan of action of non-recurrence and further awareness raising.

All significant data protection incidents will be reported through the DPO to the Information Commissioner's Office.

10.Training

The school recognises that many data protection failures are caused by ignorance and anything that promotes awareness is to be recommended. Mistakes can often be prevented by being aware that a potential problem exists and knowing who can give more detailed advice. To this end all staff (and volunteers and governors) will receive written and practical guidance on confidentiality of personal information and how this links to written policies.
Practical guidance will be provided through school CPD every three years (or earlier as required) and on an annual basis through the school's adult code of conduct. Both the training and codes of conduct will be signed for by the staff member / adult to confirm that they understand their responsibilities in relation to data protection

11. Associated Policies and Procedures:

- Third Party Data Transfer Policy
- Cloud Based Storage Policy

12. Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years.

Appendix 1 Links to resources and guidance

ICO Guidance for schools
http://ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Research_and_reports/report_dp_guidance_for_schools.ashx
A downloadable guide for schools
https://ico.org.uk/for-organisations/education/

Specific information for schools is available here
http://ico.org.uk/for_organisations/sector_guides/education

Specific information about use of Cloud Based technology
http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

Specific Information about CCTV
http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

Information and Records Management Society – Schools records management toolkit
http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school
A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/143669/handling-dbs-cert.pdf Details of storage and access to DBS certificate information.

DFE Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Appendix 2 Privacy Notice

Frogwell Primary School
Privacy Notice – Pupils

Privacy Notice (How we use pupil information)

Why do we collect and use pupil information?

We collect and use pupil information under Article 6(1)(c) of General Data Protection Regulations which provides a lawful basis for processing information where it is seen that:

"processing is necessary for compliance with a legal obligation to which the controller is subject."

Example: Regular censuses are required by the Education Act 1996 – this information can be found in the census guide documents on the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools]

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The categories of pupil-related information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Medical information
- Special educational needs information
- Exclusions/behaviour information
- Child welfare information
- Pupil outcomes and information linked to the work we undertake in school such as photographs of pupils learning activities, their work or video diaries. (these will be seen throughout school and on the school website)
- Minutes of meetings directly related to pupils.

Collecting pupil information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
We hold pupil data for only as long as the information is useful to the school and as a maximum for the duration plus one year after the child is in the school. The only exception to this is for Child Protection information which is securely stored for one year after the child has left the school or a younger sibling leaves the school.

Who do we share pupil information with?
We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority including Children's Social Care
- the Department for Education (DfE)
- school nursing
- NHS and health providers

Why we share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory

data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the school office in writing.
You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress

- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/. Further details of the school's policies and procedures relating to all of the above can be found in the school's current Data Protection Policy.

Contact:
If you would like to discuss anything in this privacy notice, please contact data protection team at: dataprotection@frogwell.wilts.sch.uk

Appendix 3 Retention Schedule

The information detailed in Appendix 3 is drawn from the IRMS Information Management Toolkit for Schools document (February 2016) This will be updated following any statutory advice or direction. For the purpose of this schedule pupil records are retained in the school which the pupil last attended until reaching statutory school age. Unless otherwise stated, this school has the responsibility for retaining these records until the pupil reaches the age of 25 years of age.

7.2 Walking Bus					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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	

1.1 Governing Body					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
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	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	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	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL

1.3 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	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	An employer's guide to right to work checks [Home Office May 2015]	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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	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] + 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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	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	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	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	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

– 2018)

4 Employers are required to take a "clear copy" of the documents which they are shown as part of this process

2.5 Payroll and Pensions					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
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					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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 Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless 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					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
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					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • 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
	Secondary		Limitation Act 1980 (Section 2)	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 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
	This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	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	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	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

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	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		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	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 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	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
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	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
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	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

2018)

6. Curriculum Management

6.1 Statistics and Management Information					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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			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. 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	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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to 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 of 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 Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
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	Limitation Act 1980 (Section 2)	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. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
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	Limitation Act 1980 (Section 2)	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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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

This section covers records created in the course of interaction between the school and the local authority.

8.1 Local Authority					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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 3 Glossary

Data Protection Act 1998: All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO The Information Commissioner's office. This is a government body that regulates the Data Protection Act.
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England: General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media: General information note from the Information Commissioner on publication of examination results.

Education Act 1996: Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005: Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998: Retention of school admission and exclusion appeal papers and other pupil records.

Appendix 4 Check Sheet

Check list for systems for handling data.

- Training for staff on Data Protection, and how to comply with requirements
- Data Protection Policy in place
- All portable devices containing personal data are encrypted
- Passwords – Staff use complex passwords
- Passwords – Not shared between staff
- Privacy notice sent to parents
- Privacy notice given to staff
- Images stored securely
- School registered with the ICO as a data controller
- Member of staff with overall responsibility for data identified (SIRO)
- Risk assessments complete
- Systems in place to ensure that data is retained securely for the required amount of time
- Process in place to allow for subject access requests.
- If school has CCTV appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed
- Paper based documents secure
- Electronic backup of data both working and secure
- Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*