EQUITAS ACADEMIES TRUST

RECORD MANAGEMENT POLICY & STAFF GUIDANCE FOR GDPR

Review Date: May 2018
To be Reviewed: May 2021
Agreed: F & GP Board
Policy Lead: Marion Lower/Pravina Patel

RECORD MANAGEMENT POLICY & STAFF GUIDANCE FOR GDPR

1. RECORDS MANAGEMENT

The Trust recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the Trust and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

2. SCOPE OF THE POLICY

This policy applies to all records created, received or maintained by staff of the Trust in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business carried out by the Trust and which are thereafter retained (for a set period) to provide **evidence of its transactions or activities. These records may be created or received,** and then stored, in hard copy or electronically.

This policy will be reviewed in line with GDPR which is due to be effective from 25th May 2018.

3. RESPONSIBILITIES

The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Headteacher.

The person responsible for records management in the Trust will give guidance about good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the school's records management guidelines.

4. RELATIONSHIP WITH EXISTING POLICIES

This policy has been drawn up within the context of:

- Freedom of Information Publication Scheme
- Data Protection Policy

5. MANAGING STUDENT RECORDS

The student record should be seen as the core record charting an individual student's progress through the Education System. The student record should accompany the student to every school they attend and should contain information that is accurate, objective and

easy to access. These guidelines are based on the assumption that the student record is a principal record and that all information relating to the student will be found in the file (although it may spread across more than one file cover).

6. FILE COVERS FOR STUDENT RECORDS

It is strongly recommended that both schools use a consistent file cover for the student record. This assists the school to ensure consistency of practice when receiving records from a number of different schools.

By using pre-printed file covers all the necessary information is collated and the record looks tidy and reflects the fact that it is the principal record containing all the information about an individual child.

7. RECORDING INFORMATION

A student or their nominated representative have the legal right to see their file at any point during their education and even until the record is destroyed (when the student is 25 years of age or 35 years from date of closure for students with special educational needs). This is their right of subject access under the General Data Protection Regulation. It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

The student record starts its life when a file is opened for each new student as they begin school. This is the file which will follow the student for the rest of his/her school career. The following information should appear on the front of the paper file:

- Surname
- Forename
- DOB
- Special Educational Needs Yes/No [This is to enable the files of students with special educational needs to be easily identified for longer retention]
- Emergency contact details
- Gender
- Preferred name
- Position in family
- UPN

On the Data Collection form the following information is accessible:

- Ethnic origin [although this is "sensitive" data under the General Data Protection Regulation, the Department for Education require statistics about ethnicity]
- Language of home (if other than English)

- Names of parents and/or guardians with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of the school, and the date of admission and the date of leaving.
- Any other agency involvement e.g. speech and language therapist, paediatrician

8. ITEMS WHICH SHOULD BE INCLUDED ON THE STUDENT RECORD

Opening a file

These guidelines apply to information created and stored in both physical and electronic format.

The student record starts its life when a file is opened for each new student as they begin school. This is the file which will follow the student for the rest of his/her school career. If pre-printed file covers are not being used, then the following information should appear on the front of the paper file:

- Surname
- Forename
- DOB
- Unique Student Number (UPN)

The file cover should also contain a note of the date when the file was opened and the date when the file is closed if, it is felt to be appropriate.

Inside the front cover the following information should be easily accessible:

- The name of the student's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family
- Ethnic origin
- Language of home (if other than English)
- Religion
- Any allergies or other medical conditions that it is important to be aware of
- Names of adults who hold parental responsibility with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of the school, admission number and the date of admission and the date of leaving.
- Any other agency involvement e.g. speech and language therapist, paediatrician

It is essential that these files, which contain personal information, are managed against the information security guidelines.

Items which should be included on the student record

- If the student has attended an early year setting, then the record of transfer should be included on the student file
- Admission form (application form)
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Photography Consents
- Years Record
- Annual Written Report to Parents
- National Curriculum and Religious Education Locally Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (this includes accident forms)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in a sealed envelope clearly marked as such)
- Child protection reports/disclosures (should be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the student

The following records should be stored separately to the student record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files before they are transferred on to another school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the student record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the student file in the event of a major incident)

9. TRANSFERRING THE STUDENT RECORD TO THE SECONDARY SCHOOL

The student record should not be weeded before transfer to the secondary school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

Primary schools do not need to keep copies of any records in the student record except if there is an ongoing legal action when the student leaves the school. Custody of and responsibility for the records passes to the school the student transfers too.

Files should not be sent by post unless absolutely necessary. If files are sent by post, they should be sent by registered post with an accompanying list of the files. The secondary school should sign a copy of the list to say that they have received the files and return that to the primary school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.

Electronic documents that relate to the student file also need to be transferred, or, if duplicated in a master paper file, destroyed.

10. RESPONSIBILITY FOR THE STUDENT RECORD ONCE THE STUDENT LEAVES THE SCHOOL

The school which the student attended until statutory school leaving age (or the school where the student completed sixth form studies) is responsible for retaining the student record until the student reaches the age of 25 years.

This retention is set in line with the Limitation Act 1980 which allows that a claim can be made against an organisation by a minor for up to 7 years from their 18th birthday.

11. SAFE DESTRUCTION OF THE STUDENT RECORD

The student record should be disposed of in accordance with the safe disposal of records guidelines.

12. TRANSFER OF A STUDENT RECORD OUTSIDE THE EU AREA

If you are requested to transfer a student file outside the EU area because a student has moved into that area the Local Authority will be contacted for further advice.

13. STORAGE OF STUDENT RECORDS

All student records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security.

Access arrangements for student records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

14. HOW LONG TO KEEP E-MAILS?

E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standard.

E-mail that needs to be kept should be identified by content; for example, does it form part of a student record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule for schools found elsewhere in the Records Management Tool Kit for Schools. These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

15. DIGITAL INFORMATION:

In order to mitigate against the loss of electronic information a school need to:

Operate an effective back-up system

You should undertake regular backups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Where possible these backups should be stored in a different building to the servers and if possible off the main school site.

This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible. Options for the management of back-up facilities include:

- Use of an off-site, central back up service (usually operated by the local authority or other provider). This involves a backup being taken remotely over a secure network (usually overnight) and stored in encrypted format in premises other than the school.
- Storage in a data safe in another part of the school premises the back-up may be stored in a fireproof safe which is located in another part of the premises. These premises must also be physically secure and any hard copy supporting data regarding the location of records should also be stored in the safe.

16. CONTROL THE WAY DATA IS STORED WITHIN THE SCHOOL

Personal information should not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff should be advised not to hold personal information about students or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, portable hard drives or even on CD.

17. MAINTAIN STRICT CONTROL OF PASSWORDS

Ensure that the data is subject to a robust password protection regime, ideally with users changing their passwords every 30 days. Discourage password sharing strongly and seek alternative ways for users to share data – like shared network drives or proxy access to email and calendars. In addition, staff should always lock their PCs when they are away from the desk to prevent unauthorised use. See appendix C on how to form and manage your password.

18. MANAGE THE LOCATION OF SERVER EQUIPMENT

Ensure that the server environment is managed to prevent access by unauthorised people.

19. ENSURE THAT BUSINESS CONTINUITY PLANS ARE TESTED

Test restore processes on a regular basis to ensure that the first time you identify a problem with the backup is not the first time you need to retrieve data from it.

20. HARD COPY INFORMATION AND RECORDS

Records which are not stored on the school's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access.

21. FIRE AND FLOOD

The cost of restoring records damaged by water can be high but a large percentage may be saved, fire is much more destructive of records. In order to limit the amount of damage which a fire or flood can do to paper records, all vital information should be stored in filing cabinets, drawers or cupboards. Metal filing cabinets are a good first level barrier against fire and water.

Where possible vital records should not be left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be seriously damaged (possibly beyond repair) in the event of a flood. The bottom shelves of a storage cupboard should be raised at least 2 inches from the ground. Physical records should not be stored on the floor.

22. UNAUTHORISED ACCESS, THEFT OR LOSS

Staff should be encouraged not to take personal data on staff or students out of the school unless there is no other alternative. If records are taken off site, staff must see the school business manager/HT and complete form. Records held within the school should be in lockable cabinets. Consider restricting access to offices in which personal information is being worked on or stored. All archive or records storage areas should be lockable and have restricted access.

Where paper files are checked out from a central system, log the location of the file and the borrower, creating an audit trail.

23. CLEAR DESK POLICY

A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/ or flood damage.

A clear desk policy involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

24. DISCLOSURE

Staff should be made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it. Ensure that where you intend to share personal information with a third party that you have considered the requirements of the General Data Protection Regulation. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing, supplying a return address which can be verified.

Where appropriate you may wish to develop a data sharing protocol with the third parties with whom you regularly share data.

25. RISK ANALYSIS

Individual schools should undertake a business risk analysis to identify which records are vital to school management and these records should be stored in the most secure manner. Reference materials or resources which could be easily replaced are more suitable for storage on open shelves or desks.

26. RESPONDING TO INCIDENTS

In the event of an incident involving the loss of information or records the school should be ready to pull together an incident response team to manage the situation. Schools should consider assigning a specific member of staff to deal with press/media enquiries.

27. MAJOR DATA LOSS/INFORMATION SECURITY BREACH

You should have a process which must be used by all members of staff if there is a major data loss or information security breach. This will involve appointing a named member of staff to liaise with the Information Commissioner's Office if an information security breach needs to be reported. In our Trust, it is the relevant Business Manager at each school who is the nominated Data Protection Officer.

Do not put off informing the Information Commissioner's Office if the incident is serious enough to justify notification. It is better to have notified the Information Commissioner before someone makes a complaint to them.

28. DISPOSAL OF DOCUMENTS:

Safe disposal of records which have reached the end of their administrative life.

NB: Please be aware that this guidance applies to all types of record, whether they are in paper or digital format.

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

The fifth data protection principle states that:

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- In each organisation, local records managers must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

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

29. SAFE DESTRUCTION OF RECORDS

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

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

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

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

- Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.
- The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction. It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.
- Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the

destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

30. FREEDOM OF INFORMATION ACT 2000 (FOIA 2000):

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

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

31. DIGITAL CONTINUITY:

The long-term preservation of digital records is more complex than the retention of physical records. A large number of organisations create data in electronic format which needs to be retained for longer than 7 years. If this data is not retained in accessible formats the organisation will be unable to defend any legal challenge which may arise.

In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 6 years should be part of a digital continuity statement.

The average life of a computer system can be as little as 5 years, however, as digital continuity is resource intensive, only records which are required to be retained for 6 years (in line with the Limitation Act 1980) or longer should be subject to digital continuity statements.

32. THE PURPOSE OF DIGITAL CONTINUITY STATEMENTS

A digital continuity statement will not need to be applied to all the records created by the school. The retention schedule should indicate which records need to be subject to a digital continuity statement. Any record which needs to be preserved for longer than 6 years needs to be subject to a digital continuity statement.

Appropriate records need to be identified as early in their lifecycle as possible so that the relevant standards can be applied to them and conversely any records which do not need to be included in the policy should also be identified in the early part of the lifecycle. Digital continuity statements should only be applied to principal copy records.

33. ALLOCATION OF RESOURCES

Responsibility for the management of the digital continuity strategy, including the completion of the digital continuity statements should rest with one named post holder. This will ensure that each information assets is “vetted” for inclusion in the strategy and that resources are not allocated to records which should not be included in the strategy.

34. **STORAGE OF RECORDS**

Where possible records subject to a digital continuity statement should be "archived" to dedicated server space which is being backed up regularly.

Where this is not possible the records should be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file or onto an external hard drive which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation.

Flash drives (also known as memory sticks) must not be used to store any records which are subject to a digital continuity statement. This storage media is prone to corruption and can be easily lost or stolen.

Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed and where appropriate added to the digital continuity policy.

35. APPROPRIATE STORAGE FOR PHYSICAL RECORDS

Records must be stored in the workplace in a way that does not cause a health and safety hazard. Records must not be stored in corridors or gangways and must not impede or block fire exits. There should be where appropriate, heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area should be secured against intruders and have controlled access as far as possible to the working space.

Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

The following are hazards which need to be considered before approving areas where physical records can be stored.

36. **ENVIRONMENTAL DAMAGE - FIRE**

Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired.

Core records should be kept in cabinets or cupboards. Metal filing cabinets will usually suffice, but for important core records, fire proof cabinets may need to be considered.

However, fireproof cabinets are expensive and very heavy, so they should only be used in special circumstances. Records which are stored on desks or in cupboards which do not have doors will suffer more damage than those which are stored in cupboards/cabinets which have close fitting doors.

37. ENVIRONMENTAL DAMAGE - WATER

Records damaged by water can usually be repaired by a specialist document salvage company. The salvage process is expensive, therefore, records need to be protected against

water damage where possible. Where flooding is involved the water may not always be clean and records could become contaminated as well as damaged.

Records should not be stored directly under water pipes or in places which are liable to flooding (either from excess rainfall or from the overflow of toilet cisterns). Records should be stored in cabinets/cupboards with tight fitting doors which provide protection from water ingress. Records stored on desks or in cabinets/cupboards without close fitting doors will suffer serious water damage.

Records should be stored at least 2 inches off the ground. Most office furniture stands 2 inches off the ground. Portable storage containers (i.e. boxes or individual filing drawers) should be raised off the ground by at least 2 inches. This is to ensure that in the case of a flood that records are protected against immediate flood damage.

Storage areas should be checked for possible damage after extreme weather to ensure no water ingress has occurred.

38. ENVIRONMENTAL DAMAGE – SUNLIGHT

Records should not be stored in direct sunlight (e.g. in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.

39. ENVIRONMENTAL DAMAGE – HIGH LEVELS OF HUMIDITY

Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records. Mould can be a hazard to human health and will damage records often beyond repair.

The temperature in record storage areas should not exceed 18oC and the relative humidity should be between 45% and 65%.

Temperature and humidity should be regularly monitored and recorded. Storage areas should be checked for damage after extreme weather conditions to reduce the risk of mould growth.

40. ENVIRONMENTAL DAMAGE – INSECT/RODENT INFESTATION

Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice).

41. RETENTION GUIDELINES:

The purpose of the retention guidelines

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use.

The retention schedule lays down the basis for normal processing under both the General Data Protection Regulation and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored.

Benefits of a retention schedule

There are a number of benefits which arise from the use of a complete retention schedule:

Managing records against the retention schedule is deemed to be "normal processing" under the General Data Protection Regulation and the Freedom of Information Act 2000. Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal relating to the request or legal hold must be stopped.

Members of staff can be confident about safe disposal information at the appropriate time. Information which is subject to Freedom of Information and Data Protection legislation will be available when required. The school is not maintaining and storing information unnecessarily.

Maintaining and amending the retention schedule

Where appropriate the retention schedule should be reviewed and amended to include any new record series created and remove any obsolete record series.

This retention schedule contains recommended retention periods for the different record series created and maintained by schools in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation and the Freedom of Information Act 2000.

Managing record series using these retention guidelines will be deemed to be "normal processing" under the legislation mentioned above. If record series are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

Using the Retention Schedule

The Retention Schedule is divided into five sections:

1. Management of the School
2. Human Resources
3. Financial Management of the School
4. Property Management
5. Student Management
6. Curriculum Management
7. Extra-Curricular Activities
8. Central Government and Local Authority

Management of the School

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

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[1]
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
	Inspection Copies[2]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

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

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

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

Please note that all information about the retention of records concerning the recruitment of Head Teachers can be found in the Human Resources section below.

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

3 School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014 p6

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

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

5 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

6 Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice

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

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	

7.2 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