

General Data Protection Regulation Policy

This policy should be read in conjunction with the equivalent Surecare Residential policy, Safeguarding, Child Protection and E-safety/Acceptable Use Policies

Created	July 2018
Last review	First Review
This review Date	July 2018
Date approved by Governors	August 2018

**At the heart of all our policies at White Trees Independent School
are the following principles:**

1. Everyone in our school can learn and achieve.
2. Everyone in our school has the potential to be successful
3. We build quality relationships with one another and everyone we work with
4. The success of our school is based on high expectations, mutual trust and respect, caring for each other and taking responsibility.
5. Our vision is to provide our students with the confidence, skills, and ambition to take the next steps towards a successful and productive life so they can contribute positively in society.

Introduction

We collect personal data about the people we deal with during the course of receiving referrals and by delivering education. This policy document sets out the approach we take towards managing this personal data to ensure we meet the data protection requirements set out in the General Data Protection Regulation (“GDPR”), any UK specific implementation of aspects of the Regulation into UK law and any guidance the Information Commissioner’s Office or the Article 29 Working Party provide.

We take data protection seriously and place a high importance on the correct and lawful processing of all personal data as well as respecting rights and privacy.

As such, this policy sets White Trees Independent School’s procedures that are to be followed, by all employees when dealing with personal data

This policy is written in line with the GDPR and with reference to; ICO, privacy notice code of practice, security of personal information, information security (principle 7), data protection obligations, individuals rights of access to examination records, the use of biometric technologies in schools, disclosure of exam results to the media, data sharing code of practice, personal information online code of practice, CCTV code of practice 2008, taking photos in schools and outsourcing guide.

Data Protection Act (DPA)

The DPA will be superseded by the GDPR on 25th May and enacted into UK law via the Data Protection Act 2018.

There is also a parental right to access educational records under ‘Education (pupil records) Regulations (NI) 1998’ Schools have 15 days to respond.

Data protection definitions

1. The GDPR defines “Personal Data” as data relating to a living individual who can be identified from those data or from other information held by, or likely to come into the possession of, the data controller. The school holds a range of personal data (including personal information about students, parents, professional records of staff members and academic information) in digital form and as paper records.
2. “Special categories of personal data” relates to more sensitive personal data including racial or ethnic origin, religious beliefs and health related information. The school will be holding various pieces of special category data such as health records relating to our students.
3. “Processing” means any activity carried out on the personal data including storage, collection, organisation and general use
4. A “Data Subject” is the person whose data it is that is being collected or processed by the Data Controller and/or the Data Processor. In school a data subject would include students, parents, teachers, etc.

5. A “Data Controller” is an organisation, such as our school, who determines the purposes of processing of data – typically this is the organisation that has collected the data in the first place and wishes to process it
6. A “Data Processor” is a person or organisation who processes data on behalf of the Data Controller (usually a third party). This will include any third party systems we use to process our data

Data Protection Principles

Under the GDPR, data controllers must adhere to a range of rules or principles. Personal data should be:

- 1) Processed fairly, transparently and lawfully.
- 2) Obtained only for one or more specified and lawful purposes.
- 3) Adequate, relevant and not excessive.
- 4) Accurate and kept up to date where necessary.
- 5) Kept for no longer than is necessary for that purpose or those purposes.
- 6) Protected by appropriate levels of security.

It is up to the Data Controller or Processor to be able to demonstrate compliance with these principles (this is the principle of “accountability”)

Lawfulness of processing

For processing to be lawful, data can only be processed when one of the following conditions apply:

- The Data Subject has given consent
- Processing is required for the performance of a contract or delivering a service
- Processing is required to comply with a legal obligation
- Processing is necessary to protect the vital interests of the Data Subject
- Processing is carried out in the public interest
- Processing is carried out in the legitimate interests of the Data Controller, but without detriment to the Data Subject

Data subject rights

Under the GDPR, Data Subjects have the following rights:

- The right to be informed (including when the data was not obtained directly from them) about who has their data, what it’s used for, who will have access to and their rights to object, withdraw consent, etc.
- The right to request whether data is being processed by the Data Controller and if so what data and how (this is a subject access request)
- The right to have their data updated and kept up to date
- The right to erasure of their data when the data is no longer needed, when consent has been withdrawn or if it has been unlawfully processed

- To restrict, in certain circumstances, the processing of their data
- The right to data portability allowing a Data Subject to request copies of their data in a format compatible with another system for their own use or to import into a third-party system
- The right to object to the processing under legitimate interests, for direct marketing purposes, for profiling or research
- The right to object to automated decision making

General Statement

We are fully committed to upholding the above principles and will:

- Inform individuals why personal information is collected.
- Notify individuals when their data is shared and explain why and with whom it was shared.
- Maintain the quality and accuracy of personal data.
- Not retain information for longer than necessary.
- Destroy any information that is no longer needed appropriately and securely.
- Protect all personal information from loss, theft and unauthorised disclosure.
- Share information with others only when legally appropriate.
- Set out procedures to ensure compliance with Subject Access Requests and other individual rights.
- Make sure all staff are fully aware of our policies.

Roles and responsibilities

All employees have a responsibility to ensure data protection compliance, however, these people have key areas of responsibility:

Directors

The Board is ultimately responsible for ensuring adequate data protection controls are in place and that

- Overall data protection compliance for the business
- Reviewing (annually) all data protection resources made available to the business, including this policy, guidance and support information
- Ensuring adequate training is in place for all employees, plus specific training for the [marketing / sales / support / customer services] teams
- Dealing with data protection and privacy related questions from any part of the business
- Dealing with subject access requests from Data Subjects (students, parents or employees)
- Dealing with any requests to access data (students, parents or employees) from external third parties, for example law enforcement and government offices
- Carrying out due diligence and ensuring appropriate contractual terms are in place for any third parties we use to share or store personal data

All employees

- All employees will familiarise themselves with this policy and any associated policies, relating to the processing of personal data and ensure their processing of personal data is within the rules set out within these policy documents. Specifically, all employees should ensure:
- All personal data accessed, used or processed during their duties is kept and processed securely
- No personal data should be disclosed verbally, in writing or by any other means to any third party, without consent from the Headteacher
- No company systems should be accessed for any reason other than for the purposes of carrying out their duties as an employee
- They contact the Directors if they are aware of an issue or are uncertain about any aspect of processing data

Fair Processing

White Trees Independent School as required by the GDPR, issue a Privacy Notice to parents/carers to inform them and their children of the purposes' for which their personal data may be held. In the case of students over 13 the notice is issued to the pupil. (Please see appendix 1 – Privacy Notice) . *Please see section 9 of this policy regarding CCTV.*

Collection of personal data

Whenever we collect data, we will only ask for data that is needed. What we collect will depend on the circumstances for which the data is to be used and this will be obvious to the individual whose data it is

Where we need consent for the purposes of processing we will:

Be open and transparent about why we are collecting the data and what is being consented to

Provide an option for the Data Subject to provide their consent

We will not provide any pre-ticked options or use any wording that could be missed or misconstrued by the Data Subject to “trick” them into consenting

We will record the place, time and situation by which that consent was given

In all circumstances, when collecting data, we will provide the following information:

Details of who we are, why we're collecting the data, what it will be used for and how long we will use and keep the data, and the legal basis for processing

Details of our Data Protection Officer and how they can be contacted

Details of the Data Subject's rights:

Data Subject access requests

Have their data corrected if details change

Have their data deleted when it is no longer needed

Object to processing

Right to complain to the Information Commissioner's Office

Details of how to withdraw consent (when consent is the lawful basis of processing)

Where we make use of data supplied by a third party, in addition to the items listed in we will also provide details of where the data came from. The information will be given to the Data Subject at the first opportunity (but not more than one calendar month from receiving the data).

Use of personal data

We will only process personal data supplied to us for its original purpose. We will not reuse the data for any other purpose unless it is lawful for us to do so (e.g. we have consent from the Data Subject).

Where “legitimate interest” is the lawful basis for processing it will be possible to demonstrate that such processing is not harmful to the Data Subject’s rights and the reason for processing as a legitimate interest, documented

Information Security

Physical Security and procedures

Staff must set strong passwords, change them regularly, and never share them. Personal data will only be accessed from password protected devices which should be locked when not in use. We will take appropriate steps to keep data storage media physically secure.

Data can be restored on request. *Please see section 9 of this policy in relation to CCTV*

7.4 Use of private computer equipment - BYOD or ‘bring your own device’

The school is responsible for school data that you process on personal devices. If you use your own device for school work you will need to ensure that you meet the responsibilities for data handling, which includes allowing access to your personal device if necessary. You must have the agreement of the Headteacher to use your own device in school and we may have to refuse some access requests for security reasons.

Security - When you use a personal device for school work you must ensure you keep personal data secure. Where appropriate and depending on the device, you will need to install the school approved software before using a personal device for school work. You should always ensure that you have set secure passwords on all your devices including mobile phones. Before using your own device in school, you need to know how to:

- prevent loss, theft or unauthorised access of data.
- keep sensitive information confidential.
- maintain the security and integrity of information.

You must delete sensitive documents including emails when you have finished working on them and make sure that you limit the amount of data that syncs to your device.

Loss and theft - If your personal device has been used for school business and is lost or stolen, you must change your password for all school services accessed from your device and report the incident to the Headteacher who will inform the Directors as soon as possible.

This may include a remote wipe of data (removing all school data from your device) and could result in the loss of any personal information stored on the device.

Some school data is highly sensitive and should never be 'stored' on a personal device. If you are unsure about what information can be stored or the protections you should use, you should ask for guidance from your line manager.

Paper based personal data

Child personal data:

- Child protection data is kept in a stand-alone locked safe bolted to a secure surface and accessible by Head Teacher and SBC only
- Exam documentation is kept in a locked exams safe in a room with no windows and is accessible by the Exams Officer only
- Student files are kept in a locked cabinet and accessible by Head Teacher and Senior Leadership Team only

Staff personal data:

- All staff personal information is kept in the HR department in a locked cabinet and accessible by HR personnel only
- Finance information is kept in a locked cabinet and accessible by finance personnel only
- Allegations in relation to members of staff is kept in a locked cabinet accessible by Directors

7.6 Acceptable Use and Expected Conduct

All School Staff are responsible for reading the e-safety/acceptable use/ICT policy including the use of mobile phones, and hand-held devices.

All students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

All Parents/Carers will provide consent for students to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to school and know and understand what the 'rules of 'appropriate use' are and what sanctions result from misuse

Accuracy of data and keeping it up to date

- If we are told by a student, parent/carer or employee that the data we hold on them is out of date or incorrect we shall make sure the incorrect data is either deleted or updated
- If we are updating information about a student we must do so immediately to ensure the old data is not processed in the meantime
- If we have shared the data with any third party, we will immediately inform the third party to ensure their copies of the data are updated

Sharing Personal Information

It may sometimes be necessary to transfer personal data to the local authority or other agencies, or for members of staff to access personal information outside of school. In these cases:

- Users must have permission to access or transfer the data out of school and use appropriately secured encrypted systems
- Devices containing personal data may only be accessed by authorised users
- Where possible, personal data should be accessed via secure remote access to the school's management information system
- Users should securely store and protect any personal devices used to access data.

The local authority should be consulted if it is necessary to transfer data to another country.

Data Retention

When doing this, the School will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

Data Protection

This policy sets out how long employment-related and student data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Retention Schedule

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule. . The retention periods are based on business needs and legal requirements.

Destruction of Records

Where records have been identified for destruction are disposed of in an appropriate way. All information is reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information are shredded before disposal wherever possible or disposed of by an appropriate waste paper merchant with confirmation that shredding has taken place. All electronic information will be deleted.

Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives.

Transferring Information to other Media

Where lengthy retention periods have been allocated to records, we will convert paper records to other media such as digital media or virtual storage . The lifespan of the media and the ability to migrate data where necessary should always be considered.

22 Website

The purpose of White Trees Independent School's website in relation to parents/carers is to help parents/carers and students view information about their school and read privacy notices.

The school will comply with the GDPR and ensure that we have parents/carers permission before taking and using images of students on the website. We will also ensure that when images are published on the website that students cannot be identified by name unless permission has been obtained upfront, as per the use of photos policy set out below.

We ensure that:

- Students are aware that all material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- Home information or individual e-mail identities are not published.
- Photographs will not identify individual students. Group shots or pictures taken over the shoulder will be used in preference to individual "passport" style.
- Full names will not be used anywhere on the Website, particularly alongside photographs.
- Written permission from parents/carers will be sought before photographs of students are published on the Website.
- Students will not be allowed to access public chat rooms.
- New facilities will be thoroughly tested before students are given access.

Photographs

Digital and video images play an important part in learning activities. Students and members of staff may use digital cameras to record activities in lessons and on school trips. These images may then be used in presentations in subsequent lessons.

Images may also be published in newsletters, on the school website and occasionally in local media. (Please see section above regarding the use of images on our website)

In line with the Information Commissioner's Office (ICO), we may take pictures for inclusion in a 'printed' prospectus or school publication without specific consent from parent/carers although we will indicate their intention.

Note: we obtain permission from parent/carers on an annual basis consenting to the use of photographs.

Training

Staff awareness is key and underpinned by eight common sense principles or points of good information practice. Staff will be requested to read and sign the data protection Policy to ensure that they understand all processes and procedures and who to pass requests onto. This policy will also form part of the annual all staff abbreviated policy training and will include:

1. What is data protection?
2. What is my schools approach to data protection?
3. Why do I need to know about data protection?
4. The main data protection principles – what are they?
5. Formal requests – how do I deal with?
6. Telephone enquiries – how do I handle?
7. Can I or should I release information?
8. Staff know what they should be doing and are doing it.

Appendix 1 – Retention Schedule

1. Child Protection					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of life of the record
1.1	Child Protection file	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years ¹	SECURE DISPOSAL
1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL
1.3	Social Care	Yes		75 years	SECURE DISPOSAL

2. Board/Governors					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of life of the record

2. Board/Governors					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of life of the record
2.1	Minutes				
	<ul style="list-style-type: none"> Principal set (signed) 	No		Permanent	Retain in school for 6 years from date of meeting
	<ul style="list-style-type: none"> Inspection copies 	No		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they should be shredded]
2.2	Agendas	No		Date of meeting	SECURE DISPOSAL
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.4	Annual Parents' meeting papers	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.5	Instruments of Government	No		Permanent	Retain in school whilst school is open
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required
2.7	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (inc if the expired policy is part of a past decision making process)
2.9	Complaints file	Yes		Date of resolution of complaint + 6 years	Retain in school for the six years Review for further retention in the case of contentious disputes SECURE DISPOSAL routine complaints
2.10	Annual Reports required by the Department for Education	No	Education (Governors' Annual Reports) (England) (Amendment)	Date of report + 10 years	

2. Board/Governors					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of life of the record
			Regulations 2002.SI 2002 No 1171		
2.11	Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years

3. Management					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
3.1	Log Books	Yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry
3.2	Minutes of the SMT and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting
3.3	Reports made by the head teacher or the management team	Yes		Date of report + 3 years	Retain in the school for 3 years from meeting
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Closure of file + 6 years	SECURE DISPOSAL
3.5	Correspondence created by head teachers, deputy head teachers, and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL

3. Management					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
3.6	Professional development plans	Yes		Closure + 6 years	SECURE DISPOSAL
3.7	School development plans	Yes		Closure + 6 years	Review
3.8	Admissions - if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL
3.9	Admissions - if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL
3.10	Admissions - Secondary Schools - Casual	Yes		Current year + 1 year	SECURE DISPOSAL
3.11	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL
3.12	Supplementary Information form including additional information such as religion, medical conditions etc.				

4. Students					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
4.1	Admission Registers	Yes		Date of last entry in the book (or for + 6 years These records are no longer generated in paper but electronically held using Scholarpack software.	Retain in the school for 6 years from the date of the last entry then consider transfer to the Archives

4. Students					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
4.2	Attendance registers	Yes		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]
4.3	Pupil Files Retained in Schools	Yes			
4.3a	• Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.3b	• Secondary		Limitation Act 1980	DOB of the pupil + 25 years ³	SECURE DISPOSAL
4.4	Pupil files	Yes			
4.4a	• Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.4b	• Secondary		Limitation Act 1980	DOB of the pupil + 25 years	SECURE DISPOSAL
4.5	Special Educational Needs files , reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. SEN files to be kept for a longer period of time to defend the school against 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.	SECURE DISPOSAL
4.6	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL

4. Students					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
4.7	Examination results	Yes			
4.7a	• Public	No		Year of examinations + 6 years	SECURE DISPOSAL
4.7b	• Internal examination results	Yes		Current year + 5 years ⁵	SECURE DISPOSAL
4.8	Any other records created in the course of contact with students	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL
4.9	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
4.11	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.12	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.13	Parental permission slips for school trips - where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
4.14	Parental permission slips for school trips - where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all students on the trip need to be retained to show that the rules had been followed for all students	SECURE DISPOSAL

4. Students					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
4.15	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	No	3 part supplement to the Health & Safety of Students on Educational Visits (HASPEV) (1998).	Date of visit + 14 years ⁶	N
4.16	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	No	3 part supplement to the Health & Safety of Students on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	N
4.17	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]

5 Curriculum					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
5.1	School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
5.3	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 new retention period or SECURE DISPOSAL

5 Curriculum					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
5.4	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.5	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.6	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.8	Students' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.9	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL
5.10	SATS records - Examination Papers and Results	Yes		Current year + 6 years	SECURE DISPOSAL
5.11	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
5.12	Value Added & Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL

5 Curriculum					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
5.13	Self-Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6. Personnel Records held in Schools					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
6.2	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL
6.4	Pre-employment vetting information (including CRB checks)	No	CRB guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]
6.5	Disciplinary proceedings:	Yes	Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your DCP for further advice.		
6.5a	• oral warning			Date of warning + 6 months	SECURE DISPOSAL
6.5b	• written warning - level one			Date of warning + 6 months	SECURE DISPOSAL
6.5c	• written warning - level two			Date of warning + 12 months	SECURE DISPOSAL
6.5d	• final warning			Date of warning + 18 months	SECURE DISPOSAL

6. Personnel Records held in Schools					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
6.5e	<ul style="list-style-type: none"> case not found 			If child protection related please see 1.2 otherwise SECURE DISPOSAL immediately at the conclusion of the case	SECURE DISPOSAL
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
6.7	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL
6.8	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year +3yrs	SECURE DISPOSAL
6.10	Records held under Retirement Benefit Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
6.11	Proofs of identity collected as part of the process of checking "portable" enhanced CRB 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	

7. Health and Safety

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
7.1	Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.2a	• Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
7.2b	• Children	Yes		DOB of child + 25 years ⁸	SECURE DISPOSAL
7.3	COSHH			Current year + 10 years [where appropriate an additional retention period may be allocated]	
7.4	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL
7.5	Policy Statements			Date of expiry + 1 year	SECURE DISPOSAL
7.6	Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SECURE DISPOSAL
7.9	Fire Precautions log books			Current year + 6 years	SECURE DISPOSAL

8. Administrative					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
8.1	Employer's Liability certificate			Closure of the school + 40 years	SECURE DISPOSAL
8.2	Inventories of equipment & furniture			Current year + 6 years	SECURE DISPOSAL
8.3	General file series			Current year + 5 years	Review to see whether a further retention period is required
8.4	School brochure or prospectus			Current year + 3 years	
8.5	Circulars (staff parents/students)			Current year + 1 year	SECURE DISPOSAL
8.6	Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required
8.7	Visitors book			Current year + 2 years	Review to see whether a further retention period is required
8.8	PTA/Old Students Associations			Current year + 6 years	Review to see whether a further retention period is required

9. Finance					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
9.1	Annual Accounts		Financial Regulations	Current year + 6 years	

9. Finance					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
9.2	Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
9.3	Contracts				
9.3a	• under seal			Contract completion date + 12 years	SECURE DISPOSAL
9.3b	• under signature			Contract completion date + 6 years	SECURE DISPOSAL
9.3c	• monitoring records			Current year + 2 years	SECURE DISPOSAL
9.4	Copy orders			Current year + 2 years	SECURE DISPOSAL
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	SECURE DISPOSAL
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
9.7	Annual Budget and background papers			Current year + 6 years	SECURE DISPOSAL
9.8	Order books and requisitions			Current year + 6 years	SECURE DISPOSAL
9.9	Delivery Documentation			Current year + 6 years	SECURE DISPOSAL
9.10	Debtors' Records		Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
9.11	School Fund - Cheque books			Current year + 3 years	SECURE DISPOSAL
9.12	School Fund - Paying in books			Current year + 6 years then review	SECURE DISPOSAL
9.13	School Fund - Ledger			Current year + 6 years then review	SECURE DISPOSAL

9. Finance					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
9.14	School Fund - Invoices			Current year + 6 years then review	SECURE DISPOSAL
9.15	School Fund - Receipts			Current year + 6 years	SECURE DISPOSAL
9.16	School Fund - Bank statements			Current year + 6 years then review	SECURE DISPOSAL
9.17	School Fund - School Journey books			Current year + 6 years then review	SECURE DISPOSAL
9.18	Student grant applications			Current year + 3 years	SECURE DISPOSAL
9.19	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
9.20	Petty cash books			Current year + 6 years	SECURE DISPOSAL

10. Property					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
10.1	Title Deeds			Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
10.2	Plans			Permanent	Retain in school whilst operational
10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
10.4	Leases			Expiry of lease + 6 years	SECURE DISPOSAL
10.5	Lettings			Current year + 3 years	SECURE DISPOSAL

10. Property					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
10.7	Maintenance log books			Current year + 6 years	SECURE DISPOSAL
10.8	Contractors' Reports			Current year + 6 years	SECURE DISPOSAL

11. Local Authority					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
11.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
11.3	Circulars from LEA			Whilst required operationally	Review to see whether a further retention period is required

12. Department for Children, Schools and Families					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
12.1	HMI reports			These do not need to be kept any longer	
12.2	OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required

12. Department for Children, Schools and Families					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
12.3	Returns			Current year + 6 years	SECURE DISPOSAL
12.4	Circulars from Department for Children, Schools and Families			Whilst operationally required	Review to see whether a further retention period is required

13. Connexions					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
13.1	Service level agreements			Until superseded	SECURE DISPOSAL
13.2	Work Experience agreement			DOB of child + 18 years	SECURE DISPOSAL

14. Schools Meals					
	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
14.1	Dinner Register			Current year + 3 years	SECURE DISPOSAL
14.2	School Meals Summary Sheets			Current year + 3 years	SECURE DISPOSAL

15. Family Liaison Officers and Home School Liaison Assistants					
	Basic file description	DP issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
15.1	Day Books	Yes		Current year + 2 years then	SECURE DISPOSAL

15. Family Liaison Officers and Home School Liaison Assistants					
	Basic file description	DP issues	Statutory Provisions	Retention Period [operational]	Action at the end of the life of the record
				review	
15.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL
15.3	Referral forms	Yes		While the referral is current	SECURE DISPOSAL
15.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
15.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	DELETE
15.6	Group Registers	Yes		Current year + 2 years	SECURE DISPOSAL

