General Data Protection Regulation Policy

Introduction

Northleigh House School (NHS) recognises and accepts it responsibility as set out in The General Data Protection Regulation 2016 (GDPR) which replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member State including the Data Protection Act 1998. Its purpose is to protect the "rights and freedoms" of natural persons (living individuals) and to ensure that the personal data is not process without their knowledge and, wherever possible, that it is processed with their consent.

The school, as a Data Controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information.

This policy statement applies to all school trustees and employees, and individuals about whom the school processes personal information, as well as other partners and companies with which the school undertakes it business. The most up to date version is available on the school website.

1. Policy Statement

The school needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, students, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material.

We regard the lawful and correct treatment of personal information by the school as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The school wishes to ensure that it treats personal information lawfully, correctly and in compliance with the GDPR.

2. Definitions

Personal Data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories of Personal Data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal Data Breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data Subject Consent – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third Party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing System – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

3. Responsibilities and Roles under the General Data Protection Regulation

3.1 NHS is a data controller and/or data processor under the GDPR.
3.2 Trustees and all those in managerial or supervisory roles at NHS are responsible for developing and encouraging good information handling practices; responsibilities are set out in individual job descriptions.
3.3 The Data Protection Officer, a role specified in the GDPR, is accountable to the trustees and senior leadership team of the school for the management of personal data within the school for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes: development and implementation of the GDPR as required by this policy; and security and risk management in relation to compliance with the policy.
3.4 The Data Protection Officer, whom the trustees and senior leadership team consider to be suitably qualified and experienced, have been appointed to take responsibility for NHS's compliance with this policy and, in particular, have direct responsibility for ensuring that NHS complies with the GDPR, as do all managers and supervisors in respect of data processing that takes place within their area of responsibility.
3.5 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure (GDPR 004) and is the first point of call for employees seeking clarification on any aspect of data protection compliance.
3.6 Compliance with the data protection legislation is the responsibility of all trustees, employees and volunteers of NHS who process personal data.
3.7 All trustees, staff and volunteers are required to have undertaken data protection awareness training, the nature of which will be decided by the frequency of processing and the nature of the personal data they may process.
3.8 Trustees, employees and volunteers of NHS are responsible for ensuring that any personal data about them and supplied by them is accurate and up-to-date.

4. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The school's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently
Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources. The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.6 Personal data must be processed in a manner that ensures the appropriate security.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability).

5. Data Subjects' Rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO to assess whether any provision of the GDPR has been contravened.

- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

5.2 NHS ensures that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure (GDPR 004)(Appendix 1).
- Data subjects have the right to complain to NHS in relation to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with NHS's standard Complaints Procedure.

6. Consent

6.1 NHS understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.
6.2 NHS understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them as consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication.
6.4 The Controller must be able to demonstrate that consent was obtained for the processing operation.
6.5 For sensitive data, explicit written consent (Consent Procedure GDPR 008) of data subjects must be obtained unless an alternative legitimate basis for processing exists.
In most instances, consent to process personal and sensitive data is obtained routinely by NHS using standard consent documents or statements on forms.

7. Security of Data

7.1 All trustees, employees and volunteers are responsible for ensuring that any personal data that NHS holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by NHS to receive that information and has entered into a confidentiality agreement.
7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy (GDPR 009). All personal data should be treated with the highest security and must be kept:

in a lockable room with controlled access; and/or
in a locked drawer or filing cabinet; and/or
if computerised, password protected; and/or
stored on computer media which are encrypted in line with Secure Disposal of Storage Media (GDPR 007). The only certain method to make data on these types of media irretrievable is physical destruction.

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised personnel. All trustees, employees and volunteers are required to follow the Acceptable Data Use Agreement (GDPR 010) if they are given access to organisational information of any sort.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day business use, they must be removed to secure archiving or securely destroyed.
7.5 Personal data may only be deleted or disposed of in line with this policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by GDPR 007 before disposal.
7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

8. Disclosure of Data

8.1 NHS must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All trustees, employees and volunteers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of NHS's business.
8.2 The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual in life and death situations.

8.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

9. Retention and Disposal of Data

Under the Freedom of Information Act 2006, 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 (Appendix 2) below 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.

Date: **September 2018**

Review Date: **September 2021**

Appendix 1

SUBJECT ACCESS REQUEST RECORD

Name of Data Subject ……..
Name of Person who made request: …….
Date request received: …….
Contact Data Protection Officer: …….
Date of acknowledgement sent: …….
Name of person dealing with request: …….

	Notes
Are they entitled to the data?	
Do you understand what data they are asking for?	
Identify the data	
Collect the data required?	
Do you own all the data?	
Do you need to exempt/redact data?	
Is the data going to be ready in time?	
Create pack	
Inform requestor you have the data	
Deliver data	

At all stages your DPO or Data Protection lead will be able to provide you with advice.

Date request completed: ……
(within 30 days of request)
Signed off by: ……

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
TRUSTEES				
Agendas for Trustees meetings	There may be data 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
Minutes of Trustee meetings Principal Set (signed) Inspection Copies	There may be data protection issues if the meeting is dealing with confidential issues relating to staff.		 PERMANENT Date of meeting plus 3 years.	 If the schools is unable to store these then they should be offered to the County Archives Service. If these minutes contain any sensitive, personal information they must be shredded.
Reports presented to the Trustees	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 retained with the signed set of the minutes.
Trusts and Endowments managed by the Trustees	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.
Action plans created and administered by the Trustees	No		Life of the action plan plus 3 years.	SECURE DISPOSAL
Policy documents created and administered by the Trustees	No		Life of the policy plus 3 years.	SECURE DISPOSAL

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
Records relating to complaints dealt with by the Trustees	Yes		Life of the policy plus 3 years.	SECURE DISPOSAL
Annual Reports	No	The Charities Act 2011 Section 162 The Charities (Accounts and Reports) Regulations 2008	Date of report plus 10 years.	SECURE DISPOSAL
Proposals concerning the change of status of the school	No		Date proposal accepted or declined plus 3 years.	SECURE DISPOSAL
HEAD TEACHER AND SENIOR MANAGEMENT TEAM				
Log books of activity in the school maintained by the Headteacher	There may be data protection issues if the log book refers to individual pupils or members of staff (accident log).		Date of last entry in the book and a minimum of 6 years then REVIEW.	SECURE DISPOSAL
Minutes of Senior Management 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 and 3 years then REVIEW.	SECURE DISPOSAL
Reports created by the Headteacher 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 and a minimum of 3 years then REVIEW.	SECURE DISPOSAL
Records created by Headteacher, School Director, Heads of Department and other members of staff with administrative responsibilities	There may be data protection issues if the records refers to individual pupils or members of staff.		Current academic year and 6 years then REVIEW.	SECURE DISPOSAL

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
Correspondence created by Headteacher, School Director, Heads of Department 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 plus 3 years then REVIEW.	SECURE DISPOSAL
Provisional Development Plans	Yes		Life of the plan plus 6 years.	SECURE DISPOSAL
School Development Plans	No		Life of the plan plus 3 years.	SECURE DISPOSAL
ADMISSIONS PROCESS				
Admissions Policy	No		Life of policy plus 3 years then REVIEW.	SECURE DISPOSAL
Admissions – if the admission is successful	Yes		This information should be added to the student file. Date of Birth of the student plus 25 years.	SECURE DISPOSAL
Admissions – if the admission is unsuccessful	Yes		Resolution of case plus 3 months	SECURE DISPOSAL
Register of Admissions	Yes		Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.	REVIEW Schools may wish to consider keeping the admission register permanently as often school receive enquiries from past pupils to confirm the date they attended the school.
Proof of address and Identification supplied by parents as part of the admissions process	Yes		This information should be added to the student file. Date of Birth of the student plus 25 years.	SECURE DISPOSAL
Supplementary information form including additional information	Yes			

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
such as religion, medical conditions etc. For successful admissions For unsuccessful admissions			This information should be added to the student file. Date of Birth of the student plus 25 years. 3 months after unsuccessful admissions.	SECURE DISPOSAL SECURE DISPOSAL
OPERATIONAL ADMINISTRATION				
General files	No		Current year plus 5 years then REVIEW.	SECURE DISPOSAL
Records relating to the creation and publication of the school brochures or prospectus	No		Current year plus 3 years.	STANDARD DISPOSAL
Records relating to the creation and distribution of circulars to staff, parents or students	No		Current year plus 1 year.	STANDARD DISPOSAL
Newsletters and other items with a short operational use	No		Current year plus 1 year.	STANDARD DISPOSAL
Visitors' Books and Signing in Sheets	Yes		Current year plus 6 years then REVIEW.	SECURE DISPOSAL
Records relations to the creation and management of Parent Teacher Associations and/or Old Students Associations	No		Current year plus 6 years then REVIEW.	SECURE DISPOSAL
RECRUITMENT				
All records leading up to the appointment of a new Headteacher	Yes		Date of appointment plus 6 years.	

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate plus 6 months.	SECURE DISPOSAL
All records leading up to the appointment of a new member of staff – successful candidates	Yes		All relevant information should be added to the Staff Personal File and all other information retained for 6 months.	SECURE DISPOSAL
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 copes of DBS certificates, just certificate number.	
Proofs of identify collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these documents should be added to the Staff Personal File.	
Pre-employment vetting information – Evidence proving right to work in the United Kingdom	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.	
Staff Personal File	Yes	Limitation Act 1980 Section 2	Termination of Employment plus 6 years.	SECURE DISPOSAL
Timesheets	Yes		Current year plus 6 years.	SECURE DISPOSAL
Annual appraisal records	Yes		Current year plus 5 years.	SECURE DISPOSAL
MANAGEMENT OF DISCIPLINARY AND GRIEVOUS PROCESSES				

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
Allegation Of a child protection nature against a member of staff including where the allegation is unfounded	Yes	"Keeping children safe in education 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.
Disciplinary Proceedings Oral Warning Written Warning 1 Written warning 2 Final Warning Case not found	Yes			SECURE DISPOSAL If warnings are placed on personal files, then they must be weeded from the file.
HEALTH AND SAFETY				SECURE DISPOSAL
Health and Safety Policy Statements	No		Life of policy plus 3 years.	SECURE DISPOSAL
Healthy and Safety risk Assessments	No		Life of risk assessment plus 3 years.	SECURE DISPOSAL
Records relating to accident/injury at work	Yes			SECURE DISPOSAL
Accident Reporting Adults Students	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Administration Act 1992 Section 8. Limitation Act 1980	Date of incident plus 6 years. Date of Birth of the student plus 25 years.	SECURE DISPOSAL

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
Control of Substances Hazardous to Health (COSHH)	No	Control of substances Hazardous to Health Regulations 2002 SI2002 No 2677 Regulation 11; Records kept under 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18(2)	Current year plus 40 years.	SECURE DISPOSAL
Fire Log Book	No		Current year plus 6 years.	SECURE DISPOSAL
PAYROLL AND PENSIONS				
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960) revised 1999 (SI1999/567)	Current year plus 3 years.	SECURE DISPOSAL
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year plus 6 years.	SECURE DISPOSAL
RISK MANAGEMENT AND INSURANCE				
Employer's Liability Insurance Certificate	No		Closure of the school plus 40 years.	SECURE DISPOSAL
ACCOUNTS AND STATEMENTS INCLYDING BUDGET MANAGEMENT				
Annual Accounts	No		Current year plus 6 years.	SECURE DISPOSAL

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
Loans and Grants managed by the school	No		Date of last payment on the loan plus 12 years then REVIEW.	SECURE DISPOSAL
Student Grant applications	Yes		Current year plus 3 years.	SECURE DISPOSAL
All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget plus 3 years.	SECURE DISPOSAL
Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year plus 6 years.	SECURE DISPOSAL
Records relating to the collection and banking of monies	No		Current financial year plus 6 years.	SECURE DISPOSAL
Records relating to the identification and collection of debt	No		Current financial year plus 6 years.	SECURE DISPOSAL
SCHOOL FUND				
School Fund – Cheque books	No		Current financial year plus 6 years.	SECURE DISPOSAL
School Fund – Paying in books	No		Current financial year plus 6 years.	SECURE DISPOSAL
School Fund - Ledger	No		Current financial year plus 6 years.	SECURE DISPOSAL
School Fund - Invoices	No		Current financial year plus 6 years.	SECURE DISPOSAL
School Fund - Receipts	No		Current financial year plus 6 years.	SECURE DISPOSAL
School Fund – Bank Statements	No		Current financial year plus 6 years.	SECURE DISPOSAL

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
PROPERTY MANAGEMENT				
Leases of property leased by or to the school	No		Expire of lease plus 6 years.	SECURE DISPOSAL
Records relating to the letting of school premises	No		Current financial year plus 6 years.	SECURE DISPOSAL
MAINTENANCE				
All records relating to the maintenance of the school carried out by contractors	No		Current financial year plus 6 years.	SECURE DISPOSAL
STUDENT'S EDUCATIONAL RECORD				
Students Educational Record required by The Education (Pupil Information)(England) Regulations 2005	Yes	The Education (Pupil Information)(England) Regulations 2005 SI 2005 No. 1437 Limitation Act 1980 (Section 2)	Date of Birth of the student plus 25 years.	SECURE DISPOSAL
Examination Results	Yes		This information should be added to the student file.	SECURE DISPOSAL
Child Protection information held on student's file	Yes	"Keeping children safe in education for schools and colleges March 2015" "Working together to safeguard children. A guide to inter-agency working to safeguard	If any records relating to children protection issues are place on the student's file, it should be in a sealed envelope and then retained for the same period of time as the student's file.	SECURE DISPOSAL – these records MUST be shredded.

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
		and promote the welfare of children March 2015"		
Child Protection information held in separate files	Yes	"Keeping children safe in education 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"	Date of Birth of the student plus 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 records.	SECURE DISPOSAL – these records MUST be shredded.
ATTENDANCE				
Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in attendance register must be preserved for a period of 3 years after the date on which the entry was made.	SECURE DISPOSAL
Correspondence relating to authorised absence		Education Act 1996 Section 7	Current academic year plus 2 years.	SECURE DISPOSAL
SPECIAL EDUCATIONAL NEEDS				
Special Educational Needs files, reviews and Individual Education Plans		Limitation Act 1980 Section 2	Date of Birth of the student plus 25 years.	SECURE DISPOSAL
Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of Birth of the student plus 25 years (This would normally be retained on the student's file).	SECURE DISPOSAL unless the document is subject to a legal hold.

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of Birth of the student plus 25 years (This would normally be retained on the student's file).	SECURE DISPOSAL unless the document is subject to a legal hold.
STATISTICS AND MANAGEMENT INFORMATION				
Curriculum returns	No		Current year plus 3 years.	SECURE DISPOSAL
Examination Results (Schools Copy) Results Examination Papers	Yes		Current year plus 6 years. Results recorded on the student's educational file will be retained until the student reaches the age of 25 years. The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
Published Admission Number (PAN) Reports	Yes		Current year plus 6 years.	SECURE DISPOSAL
IMPLEMENTATION OF CURRICULUM				
Schemes of Work	No		Current year plus 1 year.	SECURE DISPOSAL
Timetable	No		Current year plus 1 year.	SECURE DISPOSAL
Marks	No		Current year plus 1 year.	SECURE DISPOSAL
Record of Homework Set	No		Current year plus 1 year.	SECURE DISPOSAL
Student's Work	No		Current year plus 1 year.	SECURE DISPOSAL
EXTRA CURRICULAR ACTIVITIES				

Record Description	Data Protection Issues	Statutory Provisions	Retention information/period	Action at end of administrative life of the record (method of disposal)
Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip.	SECURE DISPOSAL
Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 Section 2	Date of Birth of the student involved plus 25 years. The permission slips for all the students on the trip need to be retained to show that the rules had been followed for all students.	SECURE DISPOSAL
LOCAL AUTHORITY				
Attendance Returns	Yes		Current year plus 2 years.	SECURE DISPOSAL
School Census Returns	No		Current year plus 5 years.	SECURE DISPOSAL
Circulars and other information sent from the Local Authority	No		Operational use.	SECURE DISPOSAL
CENTRAL GOVERNMENT				
OFSTED reports and papers	No		Life of the report then REVIEW.	SECURE DISPOSAL
Returns made to central government	No		Current year plus 6 years.	SECURE DISPOSAL
Circular and other information sent from central government	No		Operational use.	SECURE DISPOSAL