Lonsdale School

Data Protection Policy
(including Data Storage)

This document has been devised using the following information sources:-

1. ICO Freedom of information
   Information Commissioner's Office
   https://ico.org.uk/for-organisations/education
2. DfE data Protection and Privacy June 2014
3. Hertfordshire Grid for Learning http://www.thegrid.org.uk
4. Staff Guidance on Data Security SITSS Feb 2012
5. Essex Primary Headteachers www.essexprimaryheads.co.uk

This policy is applicable to both School and REP

Policy agreed by SLT	March 2017
Policy ratified by Governors	April 2017
ICO Data Protection certicate	December 2018
Review date:	April 2019

PART 1 STATEMENT OF INTENT

This policy is designed to help to comply with the responsibilities for information rights in schools

Lonsdale School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

Lonsdale registration number is Z8354626. It expires on the 11th December 2018.

Schools have a duty to publish a Privacy Notice to staff, pupils and parents. This does not need to be issued on an annual basis as long as new pupils/parents and staff are made aware and the documents are readily available on the school website[1].

PART 2 ORGANISATION

Purpose

This policy is intended to ensure that personal and school information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically[2].

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

[1] DfE School Census 2016-17 Guide version 1.5 www.gov.uk
[2] See Appendix 3: Data Storage Management

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

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

General Statement

School is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded[3]
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests[4]
- Ensure staff are aware of and understand policies and procedures

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact **Mrs Annemari Ottridge, Headteacher** who will also act as the contact point for any subject access requests.

[3] See Appendix 4: Staff Guidance: data security

[4] See Appendix 5: Procedures for responding to subject access requests

Appendix 1

Privacy Notice: Primary

PRIVACY NOTICE
for
Pupils in Primary Schools and Children in Early Years Settings

Privacy Notice - Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information

We will not give information about your child/children to anyone without your consent unless the law and our policies allow us to.

We are required by law to pass some information about your child/children to the Local Authority (LA) and the Department for Education. If you want to receive a copy of the information we hold or share about your child(ren), please contact the Admin Office.

If you need more information about how the LA and the DfE store and use this information, then please go to the following websites
https://www.hertfordshire.gov.uk/services/Schools-and-education/Schools-and-education.aspx

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you cannot access these websites, please contact the LA or DfE

Data Protection Team Information Governance Unit Room C1 County Hall Pegs Lane Hertford SG13 8DQ email: data.protection@hertfordshire.gov.uk	Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT Website: https://www.gov.uk/government/organisations/department-for-education Email:info@education.gsi.gov.uk Telephone: 0370 000 2288

PRIVACY NOTICE
for
Pupils of Secondary School age

Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information.

For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.

Once our pupils reach the age of 13, the law requires us to pass on certain information to Herts CC who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent/guardian can request that **only** their child's name, address and date of birth be passed to the LA by informing the Business Manager. This right is transferred to the child once he/she reaches the age 16. For more information about services for young people, please go to the local authority website https://nationalcareersservice.direct.gov.uk/aboutus/Pages/default.aspx

The Learning Records Service is operated by the Skills Funding Agency. The Learning Records Service collects data relating to learners registering for relevant post-14 qualifications, for example GCSEs and A-Levels, Entry to Employment Certificates, Regulated Qualifications Frameworks and Welsh Baccalaureate and associated units. The information you supply will be used by the Skills Funding Agency, an executive agency of the Department for Education (DfE), to issue you with a Unique Learner Number (ULN), and to create your Personal Learning Record. For more information about how your information is processed and shared refer to the Extended Privacy Notice available on Gov.UK. For more information regarding ULN and PLR data please visit:https://www.gov.uk/government/publications/learning-records-service-the-plr-for-learners-and-parents

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please contact the school Business Manager

We are required, by law, to pass certain information about our pupils to our LA and the Department for Education (DfE).

The DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract
For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received
If you need more information about how our local authority and/or DfE collect and use your information, please visit: https://www.hertfordshire.gov.uk/services/Schools-and-education/Schools-and-education.aspx or the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Appendix 2

Privacy Notice: Workforce[5]

PRIVACY NOTICE
for
School Workforce

Privacy Notice - Data Protection Act 1998

Lonsdale School is the Data Controller for the purposes of the Data Protection Act.

Personal data is held by Lonsdale School about those employed or otherwise engaged to work at school. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector
- Enabling a comprehensive picture of the workforce and how it is deployed to be built
- Informing the development of recruitment and retention policies
- Allow better financial modeling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We are required by law to pass on some of this data to:
- the LA
- the Department for Education (DfE)

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
- https://www.hertfordshire.gov.uk/services/Schools-and-education/Schools-and-education.aspx

If you are unable to access these websites, please contact the LA or DfE

Data Protection Team Information Governance Unit Room C1 County Hall Pegs Lane Hertford SG13 8DQ email: data.protection@hertfordshire.gov.uk	Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT Email: info@education.gsi.gov.uk Telephone: 0370 000 2288. Website: https://www.gov.uk/government/organisations/department-for-education

[5] Source: HfL Privacy Notice Primary April 2016

Data Retention: School Management **Appendix 3**

1.	**DATA STORAGE: Governing Body**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
1.1	GB Agenda	There may be data protection issues if the meeting is dealing with confidential staff issues relating to staff		One copy kept	Secure Disposal[6]
1.2	Minutes (signed principle set)			PERMANENT	
1.3	Reports presented to GB			Reports should be kept for a minimum of 6 years	Secure Disposal
1.4	Meeting papers relating to annual parents' meeting held under section 33 Education Act 2002		Section 33 Education Act 2002	Date of the meeting + a minimum of 6 years	Secure Disposal
1.5	Instruments of Government including Articles of Association	No		Permanent	Retained in school whilst school is open then offered to County Archives
1.6	Trusts and endowments managed by GB	No		Permanent	
1.7	Action plans created and administered by GB	No		Life of the Action plan + 3 years	Secure Disposal
1.8	Policy documents created and administered by GB	No		Life of the Action plan + 3 years	Secure Disposal
1.9	records relating to complaints dealt with by GB	Yes		Date of resolution of the complaint + a min of 6 years then review for further retention in case of contentious disputes	Secure Disposal
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

[6] Confidential waste bins or cross cut shredder

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
1.11	Proposals concerning the change of status of a maintained school including specialist status and Academies	No		Date proposal accepted or declined + 3 years	Secure Disposal
2.	**DATA STORAGE: Head and SLT**				
2.1	Log books of activity in school maintained by Head	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry + a min of 6 years then review	These could have permanent historical value so should be offered to County Archives if appropriate
2.2	SLT meeting minutes and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refer to individual pupils or members of staff		Date of the meeting + 3 years then review	Secure Disposal
2.3	Reports created by the Head or SLT	There may be data protection issues if the reports refer to individual pupils or members of staff		Date of the meeting + 3 years then review	Secure Disposal
2.4	Records created by Head, DHT, AHT 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
2.5	Correspondence created by Head, DHT, AHT 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

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
2.6	Professional Development Plans	Yes		Life of plan + 6 years	Secure Disposal
2.7	School Development Plans	No		Life of Plan + 3 years	Secure Disposal
3.	**DATA STORAGE: Admissions Process**				
3.1	All records relating to the creation and implementation of the School's Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, LA's, schools adjudicators and admissions appeal panels Dec 2014	Life of the policy + 3 years then review	Secure Disposal
3.2	Admissions – if successful	Yes		Date of admission + 1 year	Secure Disposal
3.3	Admissions – if unsuccessful	Yes		Resolution + 1 year	Secure Disposal
3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools Oct 2014 p6	Every entry in the admission register must be preserved for 3 years after the date on which the entry was made	Review School may wish to keep admission register permanently (to enable past student queries)
3.5	Admissions - casual	Yes		Current + 1 year	Secure Disposal
3.6	Proof of address supplied by parents as part of admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, LA's, schools adjudicators and admissions appeal panels Dec 2014	Current + 1 year	Secure Disposal

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
3.7	Supplementary information form including additional information such as religion, medical conditions etc. <u>For successful</u> admissions <u>For unsuccessful</u> admissions	Yes		Information should be added to pupil file Until appeals process completed	Secure Disposal Secure Disposal
4.	**DATA STORAGE: Operational Administration**				
4.1	General files	No		Current year + 5 years then review	Secure Disposal
4.2	Records relating to creation and publication of school brochure, prospectus, website	No		Current year + 3 years	Standard Disposal
4.3	Records relating to creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	Standard Disposal
4.4	Newsletters and other items with short operational use	No		Current year + 1 year	Standard Disposal
4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then review	Secure Disposal
4.6	records relating to the creation and management of PTA's and/or Old Pupils Associations	No		Current year + 6 years then review	Secure Disposal

5.	**DATA STORAGE: Recruitment**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
5.1	All records leading to the appointment of a new Head	Yes		Date of appointment + 6 years	Secure Disposal
5.2	All records leading to the appointment of new staff: Unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	Secure Disposal
5.3	All records leading to the appointment of new staff Successful candidate	Yes		All relevant information should be added to staff personal file and all other information retained for 6 months	Secure Disposal
5.4	pre-employment vetting information – DBS checks	No	DBS Update Service Employer Guide June 2014: Keeping Children Safe in Education. DofE Statutory Guidance sections 73,74 July 2015	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	
5.5	Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		These should be checked and a note kept of what was seen and what has been checked. If copies of documentation are kept this should be in the member of staff’s personal file	

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
5.6	Pre-employment vetting – evidence proving the right to work in the UK	Yes	Home Office: An Employers Guide to Work Checks May 2015	Where possible these documents should be added to 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 + not less than 2 years	
5.7	Staff Personal File	Yes	Limitation Act 1980 (Section2)	Termination of Employment + 6 years	Secure Disposal
5.8	Timesheets	Yes		Current year + 6 years	Secure Disposal
5.9	Annual appraisal records	Yes		Current year + 5 years	Secure Disposal
6.	**DATA STORAGE: Management of Disciplinary and Grievance Processes**				
6.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes		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 file and a copy provided to the person concerned	Secure Disposal These records must be shredded

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
6.2	Disciplinary Proceedings				
	oral warning	Yes		Date of warning + 6 months	Secure Disposal (If warnings are placed on personal files then they must be "weeded" from the file)
	written warning L1	Yes		Date of warning + 6 months	
	written warning L2	Yes		Date of warning + 12 months	
	final warning	Yes		Date of warning + 18 months	
	case not found	Yes		If the incident is child protection related (timings as above) otherwise dispose of at the conclusion of the case	Secure Disposal
7.	**DATA STORAGE: Health & Safety**				
7.1	Health & Safety Policy Statements	No		Life of Policy + 3 years	Secure Disposal
7.2	Health & Safety Risk Assessments	No		Life of risk assessment + 3 years	Secure Disposal
7.3	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

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
7.4	Accident reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8 Limitation Act 1980		
7.41	Adults			Date of the incident + 6 years	Secure Disposal
7.42	Children			DoB of the child + 25 years	Secure Disposal
7.5	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
7.6	Process of monitoring of areas where employers and persons are likely to have come into contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No.632 Regulation 19	Last action + 40 years	Secure Disposal

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
7.7	Process of monitoring of areas where employers and persons are likely to have come into contact with radiation	No		Last action + 50 years	Secure Disposal
7.8	Fire Precautions log books	No		Current year + 6 years	Secure Disposal
8.	**DATA STORAGE: Payroll and Pensions**				
8.1	Maternity Pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year + 3 years	Secure Disposal
8.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	Secure Disposal
9.	**DATA STORAGE: Risk Management and Insurance**				
9.1	Employers Liability Insurance certificate	No		Closure of the school + 40 years	Secure Disposal
10.	**DATA STORAGE: Asset Management**				
10.1	Inventories of furniture and equipment	No		Current year + 6 years	Secure Disposal
10.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	Secure Disposal

11.	**DATA STORAGE: Accounts and Statements including Budget Management**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
11.1	Annual Accounts	No		Current year + 6 years	Standard Disposal
11.2	Loans and grants managed by school	No		Date of last payment on the loan + 12 years then review	Secure Disposal
11.3	Student grant applications	Yes		Current year + 3 years	Secure Disposal
11.4	All records relating to the creation and management of budgets including the Annual Budget statement and back ground papers	No		Life of the budget + 3 years	
11.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	Secure Disposal
11.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	Secure Disposal
11.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	Secure Disposal
12	**DATA STORAGE: Contract Management**				
12.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	Secure Disposal

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
12.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	Secure Disposal
12.3	Records relating to the monitoring of contracts	No		Current year + 2 years	Secure Disposal
13.	**DATA STORAGE: School Fund**				
13.1	School Fund – cheque books	No		Current year + 6 years	Secure Disposal
13.2	School Fund – paying in books	No		Current year + 6 years	Secure Disposal
13.3	School Fund - ledger	No		Current year + 6 years	Secure Disposal
13.4	School Fund – invoices	No		Current year + 6 years	Secure Disposal
13.5	School Fund – receipts	No		Current year + 6 years	Secure Disposal
13.6	School Fund – bank statements	No		Current year + 6 years	Secure Disposal
13.7	School Fund – journey books	No		Current year + 6 years	Secure Disposal
14.	**School Meals Management**				
14.1	Free School Meals registers	Yes		Current year + 6 years	Secure Disposal
14.2	School Meals registers	Yes		Current year + 3 years	Secure Disposal
14.3	School Meals summary Sheets	No		Current year + 3 years	Secure Disposal

15.	**DATA STORAGE: Property Management**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
15.1	Title deeds of properties belonging to school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
15.2	Plans of property belonging to 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	
15.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	Secure Disposal
15.4	Records relating to the letting of school premises	No		Current financial year + 6 years	Secure Disposal
16.	**DATA STORAGE: Property Maintenance**				
16.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	Secure Disposal
16.2	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

17.	**DATA STORAGE: Pupil's Educational Record**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
17.1	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 primary school	The file should follow the child when they leave primary. This includes • To another primary • To a secondary • To a PRU • If the pupil dies whilst at primary the file should be sent to LA to be retained for statutory period • If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be sent to the LA to be retained for the statutory retention period[7]
	Secondary		Limitation Act 1980 (Section 2)	DoB of the pupil + 25 years	Secure Disposal

[7] Primary schools do not usually have sufficient storage. Records are more often requested from the LA

	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
17.2	Examination Results	Yes			
	Public	Yes		Information should be added to pupil file	Uncollected certificates should be returned to exam board or disposed of as defined by the exam board regulations
	Internal	Yes		Information should be added to pupil file	
18.	**DATA STORAGE: Child Protection**				
18.1	Child Protection information held on pupil file	Yes	Keeping Children Safe in Education. DofE Statutory Guidance 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
18.2	Child Protection information held in separate files		Keeping Children Safe in Education. DofE Statutory Guidance 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	Secure Disposal These records must be shredded

19.	**DATA STORAGE: Attendance**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
19.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools Oct 2014	Every entry in the attendance register must be preserved for a period of 3 years after the date on which the entry was made	Secure Disposal
19.2	Correspondence relating to authorised absence	Yes	Education Act 1996 Section 7	Current academic year + 2 years	Secure Disposal
20.	**DATA STORAGE: Special Educational Needs**				
20.1	SEN EHCP	Yes	Limitation Act 1980 Section 2	DoB of pupil + 25 years	Review Note: This retention period is the minimum that any pupil file should be kept
20.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to that statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	DoB of pupil + 25 years	Secure Disposal unless the document is subject to a legal hold
20.3	Advice and information provided to parents regarding educational needs	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 2	DoB of pupil + 25 years	Secure Disposal unless the document is subject to a legal hold
20.4	Accessibility Strategy	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 14	DoB of pupil + 25 years	Secure Disposal unless the document is subject to a legal hold

21.	**DATA STORAGE: Curriculum Management: Statistics and Management Information**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
21.1	Curriculum returns	No		Current year + 3 years	Secure Disposal
	Examination Results (Schools Copy)	Yes		Current year + 6 years	Secure Disposal
	SATS records -	Yes			
	Results	Yes		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. School may wish to keep a composite record of whole year SAT results. These can be kept for current year + 6 years to allow for suitable comparison	Secure Disposal
	Examination papers	No		Exam papers should be kept until any appeals/validation process is complete	Secure Disposal
21.2	PAN reports	Yes		Current year + 6 years	Secure Disposal
21.3	Value Added and Contextual Data	Yes		Current year + 6 years	Secure Disposal
21.4	SEF	Yes		Current year + 6 years	Secure Disposal

22.	**DATA STORAGE: Implementation of Curriculum**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
22.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each academic year and allocate a further retention period or Secure Disposal
22.2	Timetable	No		Current year + 1 year	
22.3	Class Record Books	No		Current year + 1 year	
22.4	Mark Books	No		Current year + 1 year	
22.5	Record of Homework set	No		Current year + 1 year	
22.6	Pupils' work	No		School may return work to pupil or – Current year + 1 year	Secure Disposal
23.	**DATA STORAGE: Ex-Curricular Activities**				
23.1	Records created by schools to obtain approval to run an Educational Visit outside the classroom	No	Outdoor Education Advisers' Panel national guidance www.oeang.info Section 3 Legal Framework and Employer Systems Section 4 Good Practice	Primary Date of visit + 14 years Secondary Date of visit + 10 years	Secure Disposal
23.2	Parental consent forms for trips where there has been no incident	Yes		Conclusion of the trip	Secure Disposal
23.3	Parental consent forms for trips where there has been an incident	Yes	Limitation Act 1980 (Section 2)	DoB of the pupil(s) involved + 25 years. Consent forms for all the pupils need to be retained to show that "rules" had been followed for all those on the trip	

24.	**DATA STORAGE: Family Liaison**				
	Basic file description	**Data Protection issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at end of administrative life of record**
24.1	Day Books	Yes		Current year + 2 years then review	
24.2	Reports for outside agencies	Yes		Whilst child is attending school	Secure disposal
24.3	Referral forms	Yes		Whilst the referral is current	
24.4	Contact data sheets	Yes		Current year then review. If contact is no longer active – remove	Secure Disposal
23.5	Contact database entries	Yes		Current year then review. If contact is no longer active – remove	Secure Disposal
23.6	Group Registers	Yes		Current year + 2 years	Secure Disposal

Appendix 4

Staff Guidance - Data Security in Schools - Dos and Don'ts

TO BE ISSUED TO ALL STAFF

Introduction

This document has been adapted from the Becta document 'Data Security – Dos and Don'ts'* as a guide for anyone working in a school who collects, manages, transfers or uses information about learners, staff or other individuals during the course of their work. The aim of this guide is to raise awareness on safe handling of data, data security, roles and responsibilities and where potential breaches of security could occur. Following these principles will help you to prevent information from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation your school might suffer if you lose sensitive information about individuals.

Your roles and responsibilities

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be aware of the risks and threats and how to minimise them.

Important 'Dos'

- make sure all staff are adequately trained
- follow guidance
    - become more security aware
    - encrypting
    - labelling
    - transmitting
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents
- read the School Policy for ICT Acceptable Use

Why protect information?

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Who is responsible and what data handling changes are required?

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team. At Lonsdale the Headteacher holds this responsibility.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. Your school should have someone who is responsible for working out exactly what information needs to be protected. This person will be known as the Information Asset Owner. They should understand what information you need to handle, how the information changes over time, who else is able to use it and why. At Lonsdale the Headteacher holds this responsibility.

The handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

The person who creates a document becomes the owner of the document and is responsible for its protection but ultimately the school has overall responsibility to protect data.

The role of the owner of a document is to understand:

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed off

Things you can do to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don't' will apply to how you handle your own personal information and will help you protect your own privacy.

Passwords

Do

- follow your school's password policy
- use a strong password (strong passwords are usually 8 characters or more and contain upper and lower case letters, as well as numbers and special characters)
- make your password easy to remember, but hard to guess.
- choose a password that is quick to type
- use a mnemonic to help you remember your password
- change your passwords if you think someone may have found out what they are
- change your passwords on a regular basis

Don't

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message

Create Strong Passwords

Strong passwords are important protections to help you have safer online transactions. The key to password strength is length and complexity

- An ideal password is long and has letters, punctuation, symbols, and numbers
- Whenever possible, use at least 14 characters or more
- The greater the variety of characters in your password, the better
- Use the entire keyboard, not just the letters and characters you use or see most often
- Create a strong password you can remember

There are many ways to create a long, complex password. Here is one way that may make remembering it easier:

What to do	**Suggestion**	**Example**
Start with a sentence or two (about 10 words total).	Think of something meaningful to you.	Long and complex passwords are safest.
Turn your sentences into a row of letters.	Use the first letter of each word.	lacpasikms (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	lACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	lACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?lACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?lACpAs56IKMs" (14 characters)

Storing personal, sensitive, confidential or classified information

Do

- ensure removable media is purchased with encryption[8]
- store all removable media securely
- securely dispose of removable media that may hold personal data
- encrypt all files containing personal, sensitive, confidential or classified data
- ensure hard drives from machines no longer in service are removed and stored securely or wiped clean so that data cannot be restored. (see section on disposal of ICT equipment ICT Acceptable Use Policy
- ensure hard copies of personal data are securely stored and disposed of after use
- ensure that documents containing sensitive or personal data are correctly labelled
- ensure that hard copies of confidential data are securely transported and stored when removed from school

Sending and sharing

Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure
- ask third parties how they will protect sensitive information once it has been passed to them
- encrypt all removable media (USB memory drives, CDs, portable drives) that is removed from your school or sent by post or courier

TrueCrypt is a free and open-source encryption software package for Windows Vista/XP, Mac OS X, and Linux platforms. [http://www.truecrypt.org/] For more information http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

The recommended approach for encryption on USB portable drives is to purchase memory sticks that have pre-installed encryption software.

Don't

- send sensitive information (even if encrypted) on removable media (USB memory drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted
- place protective labels on outside envelopes; use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information
- assume that third party organisations know how your information should be protected

[8]Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it.

Labelling sensitive information

It is good practice to label sensitive information, this will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if sensitive information is combined into a report and printed.

HCC recommend 3 levels of labelling

- Unclassified – this will imply that the document contains no sensitive or personal information and will be a public document
- Protect – this should be the default setting and be applied to documents containing any sensitive or personal data. Marking documents as Protect will demonstrated an awareness of the Data Protection Act and the school's responsibilities
- Restricted – documents containing any ultra sensitive data for even one person should be marked as Restricted
- HCC is currently reviewing software which will automatically label documents on creation

Most learner or staff personal data that is used within educational institutions will come under the PROTECT classification with a caveat.

Protect and cavetti classifications that schools may use are;

- PROTECT – PERSONAL e.g. personal information about and individual
- PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
- PROTECT – LOCSEN e.g. for local sensitive information
- PROTECT – STAFF e.g. Organisational staff only
- RESTRICTED – STAFF e.g. A large amount of data (information on over 20 persons)
- RESTRICTED – PUPILS e.g. A large amount of data (information on 20 persons)

Information containing Student UPN

A "printed individual education plan (IEP) must be classified at IL3-Restricted because it contains the pupil's unique pupil number (UPN), a data element by itself classified as IL3-Restricted."

Email and messaging

Do

- read the protocols and guidance on the grid http://www.intra.thegrid.org.uk/eservices/email/protocols/index.shtml
- report any emails that are not blocked or filtered which are seriously offensive, threatening or possibly illegal to HGfL helpdesk on 0800 052 1386
- report phishing [9] emails to the organisation they are supposedly from
- use your school's contacts or address book. This helps to stop email being sent to the wrong address
- only use your school email account for any school business, not your personal account such as Yahoo or Hotmail

[2] Phishing is an attempt to obtain your personal information (for example bank details) by sending you an email that appears to be from a trusted source (for example, your bank). Banks will never request any personal information from you via email.

[http://www.google.co.uk/search?q=define%3A+phishing].

- the document containing the information must be encrypted and the name of the individual is not to be included in the subject line. This provides additional security
- be wary of links to websites in emails, especially if the email is unsolicited

Don't

click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on

turn off any email security measures that your IT team has put in place or recommended

email sensitive information unless you know it is encrypted. Talk to your IT support for advice

try to bypass your school's security measures to access your email offsite, for example forwarding email to a personal account

Reply to chain e-mails

Please refer to the document entitled 'How to Encrypt Files' for further advice on the file encryption available on the grid at

http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

Working online

Do

- Make sure that you follow your school's policies on keeping your computers up-to-date with the latest security updates.
- Make sure that you keep any computers that you own up-to-date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT support if you need help
- Only visit websites that are allowed by your school. Remember your school may monitor and record (log) the websites you visit
- Turn on the 'Automatic Phishing Filter' available in your Microsoft Internet Explorer web browser. (Turn on attack and forgery site warnings in Mozilla Firefox if you are using this as your web browser)
- Make sure that you only install software that your IT team has checked and approved
- Be wary of links to websites in emails, especially if the email is unsolicited
- Only download files or programs from sources you trust. If in doubt talk to your IT support
- Check that your school has an acceptable internet use policy and ensure that you follow it

Laptops or Workstations

Do

- make sure that only approved software is installed on machines
- shut down your laptop or workstation using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information
- turn off and store your laptop securely, for example, if travelling use your hotel room's safe or temporarily lock in the boot of your car
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop or workstation unattended
- make sure your laptop, if it is likely to contain personal or sensitive data, is protected with encryption software
- use good password practices e.g never keep your id and password details with your laptop
- only download files or programs from sources you trust

(TrueCrypt is a free and open-source encryption software package for Windows Vista/XP, Mac OS X, and Linux platforms. [http://www.truecrypt.org/]
For more information please visit
http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

Don't

- store remote access tokens with your laptop
- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots. They are not secure.
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot
- let unauthorised people use your laptop
- use hibernate or standby

Working onsite

Do

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft
- make backup copies and protect them the same as the originals

Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room

Working offsite

Do

- only take information offsite if you are authorised to do so and only when necessary. Ensure that it is protected offsite in the ways referred to above
- wherever possible access information remotely instead of taking it offsite
- be aware of your location and take appropriate action to reduce the risk of theft
- try to reduce the risk of people looking at what you are working with
- leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies)
- ensure only authorised staff are allowed to remove data from the school's premises

Don't

- write down or otherwise record any network access information. Any such information that is recorded must be kept in a secure place and disguised
- disclose login IDs, PINs and other dial-up information to unauthorised users

Further help and support

Your organisation has a legal obligation to protect sensitive information. For more information visit the website of the Information Commissioners Office http://www.ico.gov.uk/

http://www.thegrid.org.uk/eservices/safety/policies.shtml

- Advice on esafety
- Data Handling Procedures in Government
- HMG Security Policy Framework
- Keeping data safe, secure and legal
- Dos and Don'ts
- Information risk management and protective markings
- Data encryption
- Audit logging and incident handling
- Secure remote access

http://webarchive.nationalarchives.gov.uk/20110130111510/http://www.becta.org.uk[10]

Further guidance - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

Test your online safety skills http://www.getsafeonline.org

School's toolkit Record Management Society website - http://www.rms-gb.org.uk/resources/848

[10] Full Becta guidance & documents are available using this link. Although this organisation closed in 2011, the website still contains useful information

Appendix 5

Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information

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

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

Requests for information must be made in writing; which includes email, and be addressed to **Mrs A Ottridge, Headteacher.** If the initial request does not clearly identify the information required, then further enquiries should be made.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement *(This list is not exhaustive*)

Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

School may make a charge for the provision of information, dependant upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any detail contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**.
However the 40 days will not commence until after receipt of fees or clarification of information sought.

The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

1. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

2. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

3. If there are concerns over the disclosure of information then additional advice should be sought.

4. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

5. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

6. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.
Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Mrs A Ottridge, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.org.uk