



Brindishe  
Federation

# Brindishe Federation

## Data Protection Policy

Document status	
Author	EHT, HoS, Governors, FASWO
Creation	01.05.19
Version	1
Reason for review	Yearly
Date of next review	September 2024
Approval Body	Board of Governors
Publication approval	October 2023

All Brindishe Schools collect and use personal information about staff, students, parents or carers and other individuals who come into contact with the school. This information is gathered in order to enable us to provide education and other associated functions. There may also be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

In collecting, processing, sharing, disposing and disclosing personal data, Brindishe Green, Brindishe Manor and Brindishe Lee respect responsibilities and are aware of our duties by adhering to the principles set out in the General Data Protection Regulation 2016.

The Information Commissioner's Office enforces the Regulation, issues relevant guidance and registers personal data sets held by any organisation.

As a data controller, each school must register itself with the Information Commissioners Office (ICO) annually.

All staff, Governors, volunteers, students, and agency staff will ensure that all personal data is treated confidentially. And understand failure to adhere to the policy could lead to disciplinary action.

This document sets out the school's policy for compliance with the General Data Protection Regulation (GDPR).

### **Purpose**

This policy is intended to ensure that personal information and data is dealt with and handled correctly and securely in accordance the General Data Protection Regulation 2016, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored, transported and destroyed, and irrespective of whether it is held in paper files or electronically.

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.

### **The Six Guiding Principles**

The General Data Protection Regulation 2016 establishes six enforceable principles and Brindishe schools collectively as a registered Data Controller under the Act, will comply with these principles below:

- 1** Personal data shall be processed lawfully, fairly and in transparently in relation to the data subject.
- 2** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- 3** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 4** Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 5** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- 6** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR creates a single framework for access to personal information about living individuals held in both paper and electronic form.

See Schools guidance on what to do when a Subject Access Request (SAR) is received.

## 1. Differences in data sets

Personal and Special Categories data is any information – held manually or electronically – which relates directly to a living individual.

### **Personal Data-**

This can include but is not limited to:

- Name and Address
- Contact Number
- E-mail address
- Date of Birth

### **Special Categories of Data-**

This includes data under the following headings:

- Race or ethnic origin
- Political opinion/s
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Genetic and Biometric data
- The commission or alleged commission of offences, court sentences or allegations under investigation

While not legally special category of data the following should be given special consideration whilst processing

- Qualifications
- Income level
- Employment history
- Bank Details

## 2. Roles and Responsibilities

All information collected, and records created by a Brindishe School is and remains the property of the school, not any individual, and must not be used for any activity or purpose other than the school's official business – which is education. Staff must not access or use data for their own means or personal use or give it to anyone else for their use (e.g. to parents who wish to organise a birthday party).

The Executive Head of Brindishe Schools is responsible for ensuring that each school's Headteacher carries out their responsibilities and duties.

It is everyone's responsibility to report a known loss of personal and/or sensitive information to a senior member of staff immediately.

### Head Teacher

- Responsible for ensuring all senior staff and the school are compliant with the General Data Protection Regulation

### Data Protection Officer

- Our DPO is Mr Stephen Williams, Head of Information Security and Governance | DPO. He can be contacted on either [Stephen.Williams@lewisham.gov.uk](mailto:Stephen.Williams@lewisham.gov.uk) or 0208 314 6212
- Must be in a position to undertake their tasks independently – report to Head Teacher directly
- Be point of contact for public for data protection issues
- Be involved in timely manner in all data protection issues
- Inform and advise the school, processors and employees of obligations
- Monitor data protection compliance
- Advise as required on Data Protection Impact Assessments
- To co-operate with supervisory authority, Information Commissioner's Authority (ICO)
- To act as contact point for the supervisory authority (ICO)
- Have due regard to the risk associated with processing, taking account of nature, scope and context of processing.

### School Business Manager

- Maintaining the notification of registration for Brindishe schools with the Information Commissioner's Office on an annual basis

## Head Teacher & School Business Manager

- Providing guidance to ensure all staff are aware of their data protection responsibilities under the act
- Responsible for managing and reporting data breaches to the schools data protection advisor
- Providing guidance to process Subject Access Requests and Freedom of Information requests
- Ensuring appropriate and adequate training is available to staff
- Ensuring staff are compliant with this policy and any associated procedures

## ICT Manager & School Business Manager

- Regular review of physical security of buildings and storage systems in our schools. This includes storage of paper records and the equipment used to store and process information electronically.
- Ensure all personal and sensitive data held on our management information system is backed up and held securely off- site.

## All Staff

- All staff have a responsibility to abide by the principles of the Data Protection Act. Any breach of this policy could lead to disciplinary action being taken.
- All portable electronic devices must be kept on and off school premises. If they contain personal information, they are kept securely (lockable cabinets) when not in use and access to them is restricted.
- Any personal or sensitive data taken off site should be held securely while in use and if necessary returned to school or subsequently shredded after use.
- Any confidential information on paper must be shredded after use; electronic memories professionally wiped clean or destroyed
- Staff using **personal** devices must not take, store, or share (with others or from a school to home device), photographs or personal or sensitive information about children or their families, this includes emails, texts or use of social media.

## Online Suppliers

Legislation known as the Children's code went live September 2021. The Children's Code (or Age Appropriate Design Code to give its formal title) is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. This legislation is aimed at the supplier (eg the software provider) and not the schools. The areas that software providers will have to consider / implement are:

- Mapping what personal data is collected from UK children.
- Checking the age of the people who visit their website, download their app or play their games
- Switching off geolocation services that track where in the world their visitors are.
- Not using nudge techniques to encourage children to provide more personal data.

- Providing a high level of privacy by default.

As a school we are not responsible for these checks, however as the data controller we are responsible for questioning the provider that they have complied with the new standards that the legislation is built upon in order to keep children safe when on line. This will be built in to the Data Protection Impact Assessment that is carried out when signing up to a new provider.

### 3. Processing Personal Data

Employees of Brindishe schools, when working with personal data, will adhere to the following:

- Only collect data necessary to carry out the purpose that the task relates to.
- Ensure papers containing confidential personal information are stored securely and are not left in general view in public areas. We all adopt a 'clear desk' policy.
- Respond to requests for access to personal data within 30 calendar days (See *Schools' Guidance* on access requests)
- Treat all personal information with equal respect for confidentiality and security whether in written, spoken or electronic form.
- Sharing of personal or sensitive data with/without informed consent. Where appropriate, the school may share information without consent if, in the school's judgement, there is a good reason to do so, such as the safety and well-being of the child/children involve and others who may be affected.
- Only use third parties to collect and process school's data where appropriate sharing agreements are in place, ensuring the protection of the data.
- Only retain personal data for a specified time period defined by the Schools' Retention Schedule. (See specific schools' guidance on retention)
- Do not delay data sharing where it is necessary to protect the vital interests of any individual.
- Seek approval from senior management before disclosing information for research purposes

### 4. Privacy Notices

Principle 1 of the Data Protection Act states that all personal data will be processed fairly and lawfully, and Principle 2 states that personal data shall be obtained for specified and lawful purposes.

Brindishe Schools is committed to processing personal data fairly and lawfully and have a written Fair Processing statement/Privacy Notice visible and easily accessible from the school office explaining to individuals how we will collect and process their data.

Having this statement/notice publicly available means that any individual will be able to read it before completing a data collection form (paper or electronic), and therefore will know exactly why the data is being collected and for what specific purpose/s.

The Privacy Notice includes the identity of the data controller (the school), what the data is being used for, whether the data will or may be used for any other purposes, and any extra information which will help the individual to understand how their data is used in line with data protection. The Privacy Notice should be provided the time the information is obtained from the individual if it's collected directly from the data subject. If it isn't collected directly from the data subject then it should be provided within a reasonable period of having obtained the information (maximum one month). If the information is used to communicate with the data subject, the latest it can be is when the first communication takes place. If disclosure to another party was unforeseen, then the Privacy Notice must be provided before the information is disclosed. If personal data is processed for a new reason/purpose at a later date an updated Privacy Notice must be provided.

Access to the Privacy Notice is available any time via the school office and will be referred to at the time information is requested about an individual. If disclosure to another party was unforeseen, then the Privacy Notice will be provided before the information is disclosed.

In general terms, a Privacy Notice should tell individuals the following about the school:

- Who we are & where we are based in the UK
- For what we are going to use their data
- With whom will we share individual's data
- Individual's Rights to accessing their own data including the fact that the Data Subject can complain to The Information Commissioner
- How we will keep individual's data secure and protected
- Identity & contact details of the School's Data Protection Officer
- The retention period for the data
- Any legal or contractual requirement to provide the information; plus the impact of not providing the data
- Automated decision making, with information about the consequences

A Privacy Notice should be genuinely informative and clear enough for children to understand so the school can be transparent and give individuals reassurance that they can trust the school with their personal data.

## 5. Information Sharing

The Brindishe Schools understands that it is most important that people remain confident that their personal information is kept safe and secure, and that the school maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that the school can share information appropriately as part of their day-to-day practice while protecting data when sharing.

Third Party organisations must follow the specific Information Sharing Agreements (ISAs) set out by the Brindishe Schools when sharing data. ISAs provide a framework for the secure and confidential obtaining, holding, recording, storing and sharing of information between the school and third parties.

Before entering into new data sharing agreements a Data Protection Impact Assessment (DPIA) must be completed and approved by the Data Protection Officer.

Robust IT security systems and measures must be in place to protect the school's electronic data and its IT infrastructure from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Please refer to the school's ISAs for protocols on information sharing.

See IT security policy for protecting information electronically and the records management policy for handling paper documentation.

## 6. Information Requests

There are two different information requests:

- **Subject Access Requests (SARs)**

Individuals have the right to ask for access to their information which can include factual information, expressions of opinion, and the intentions of the school in relation to them, irrespective of when the information was recorded.

There are two distinct rights of access to the information schools hold about pupils:

- **Right to the educational record**  
Under the Education (Pupil Information) (England) Regulations 2005, a parent or legal guardian has the right to access their child's educational record.
- **Subject access right**  
Under the General Data Protection Regulation 2016, a pupil has a right to see their own information. A parent or legal guardian may also make a request on behalf of their child.

If a pupil or parent makes a request for educational records, the school must respond within 15 school days. Fees for these requests will depend on the number of pages of information supplied. (For more information ask at the schools business manager)

If a pupil or parent makes a subject access request for personal information, the school must respond promptly and at most within 30 calendar days. Schools will be unable to charge for most Subject Access Requests

Requests made containing both educational and personal records, will be dealt as stated above: the educational part within 15 school days and personal within 40 calendar days.

If the Police make a request to review the CCTV a SAR must be completed and Logged (under section 2 of DPA 2018) and include the Police ref number as the reference

- **Freedom of Information Requests (FOI's)**

The Freedom of Information Act 2000 (FOIA) provides public access to information held by schools. It does this in two ways: schools are obliged to publish certain information about their activities; and, members of the public are entitled to request information from schools.



Brindishe Schools will comply with Freedom of Information requests and release non personal and non confidential information held by the school, after applying any relevant exemptions to protect certain categories of data.

The Act requires that all requests must be in writing (to include letters, faxes and e-mails). Requests must state clearly what information is required and must provide the name of the person with an address for correspondence.

On receipt of a FOI request, a school must respond promptly and in any event within 20 working days.

See Freedom of Information guidance for details.

(For help and advice in responding to an FOI request, contact the schools data protection advisor)

## • Appeals & Role of the ICO

In the event of a complaint or challenge regarding an information request response, whether this is a SAR or an FOI, the initial request, decision audit trail, correspondence and information released will be reviewed.

If the requestor is dissatisfied with the appeal outcome they may seek an independent review by the Information Commissioner.

The Information Commissioner is an independent official appointed by the Crown to oversee the General Data Protection Regulation and has the authority to demand disclosure.

In the first instance however the Information Commissioner will usually expect that individuals will have taken the matter up first with the School.

Brindishe Schools will comply with all notices and guidance issued by the Information Commissioner.

## 7. Rights of Individuals

Individuals also have the right to:

- Have personal data rectified if it is inaccurate or incomplete.
- Request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Request the suppression of processing of personal data
- Move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability
- Object to processing of data unless you can demonstrate compelling legitimate grounds for the processing
- Object to automated individual decision-making, including profiling

## 8. Dealing with breaches of the GDPR

Brindishe Schools holds personal and sensitive data relating to employees, children and their families.

Every care must be taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, we will take appropriate action to minimise any associated risk as soon as possible.

## **What is a data breach?**

Inadvertent breaches of confidentiality can occur. The following are examples and not limited to;

- Reading confidential files when there is no requirement to do so
- Giving excessive information out when less would suffice
- Sending information in error eg.to a wrong email address
- Files/records removed from the office and lost
- Unencrypted devices used and lost containing personal/sensitive details
- Information that hasn't been redacted correctly before publishing

Known breaches in confidentiality must be reported to the Headteacher immediately so it can be recorded and a formal investigation carried out.

## **What to do when a breach occurs:**

There are four elements in dealing with a data breach. These are:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

See the schools Data Breach Process for more information in the event of a data breach.

## **9. Training**

Brindishe Schools will provide annual training for all staff so they are fully aware of their obligations and responsibilities under the Data Protection Act.

## **10. Confidentiality**

Brindishe Schools must ensure that all personal data is treated confidentially. All staff must comply with the Schools Data Protection Policy, Information Security Policy, Records Management Policy, Subject Access Request Process, Freedom of Information Request Process and Data Breach Process.

## **11. What happens if this policy is breached?**

Failure to adhere to this or any related policy, could lead to disciplinary action. If any electronic devices are lost and therefore data is breached, the employee will be expected to replace the device.

## **12. Review**

Brindishe Schools' senior staff will meet with the Schools' Data Protection Officer for Lewisham on a regular basis where any records management tasks, ideas & issues will be discussed.

The Schools' Data Protection Officer for Lewisham will provide advice, guidance and training to the schools as and when needed and is available to answer questions from 9am-5pm Monday to Friday on **0208 314 9928** or e-mail [schoolsdpo@lewisham.gov.uk](mailto:schoolsdpo@lewisham.gov.uk)

## Appendix 1

### SUBJECT ACCESS REQUEST FORM

First name(s):

Family name:

Former family name (if applicable for finding data):

Mr / Mrs / Ms / Miss:

Present address:

Postcode:

Phone number:

Mobile number:

E-mail address:

If you have lived at the above address for less than two years (see guidance notes)

Previous address:

Postcode:

### Details of the information you require

#### Proof of Identification (if applicant is not known to the school)

Documents/identification supplied (*See note in guidance section*).

**Please note that the above information will be recorded for administrative purposes and may be used for statistical analysis**

### Payment

A charge maybe made if this request is excessive. The completed application form and supporting proof of identity should be taken or sent to the school office.

Signature (of applicant) ..... Date .....

.....

**For office use only:** *Fee, if necessary: £ .....Cheque/cash.*

Date request accepted .....

Date reply required by ..... (within 30 calendar days of request acceptance or 15 School days for parent/carer's own child school record).

Date reply sent .....

#### Guidance notes:

1. **Personal details:** Please complete your personal details as requested. Please tell us if you have been previously known by any other name and if you have lived at your present address for less than two years, your previous address. If you are requesting historical information then provide as many details as possible; for example, previous addresses with dates. Use a separate sheet of paper if required. Depending on data required we may need additional information such as national insurance number and date of birth.
2. **Details of the information you require:** You should give as much assistance as you can about particular areas to search so that we can give you what you require without further correspondence.
3. **Proof of identification:** If you are not known personally to us, proof of name and address is required to ensure we only give information to the correct person. We require two original pieces of documentation, for example, a recent utility bill, bank statement (photocopies are not acceptable) showing your name *and* address. In some cases additional details such as a passport or photo ID driving licence may be required due to the sensitive nature of information held. Release of financial, social care or education records will normally require this additional information.
4. **Keep your documents secure:** Always send important documents by recorded / special / registered delivery as appropriate. The School cannot be held liable for items lost in the post.
5. **Payment:** If the request is excessive, there maybe a fee. The fee is not refundable if the result of the search shows that there is no information to be supplied.



# **DESTRUCTION OF RECORDS BOOKLET**

Containing information to assist schools in planning the destruction of records, in compliance with principle 5 of the Data Protection Act 1998.

## 1.1 Table of Contents

RM Register.....	
CHILD PROTECTION.....	
Child protection files.....	
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded .....	
GOVERNORS.....	
Minutes .....	
Agendas.....	
Reports .....	
Annual parent meeting papers .....	
Instruments of Government .....	
Trusts and Endowments .....	
Action Plans .....	
Policy documents .....	
Complaint files .....	
Annual Reports required by the Department for Education .....	
Proposals for schools to become, or be established as Specialist Status schools .....	
MANAGEMENT .....	
Log books.....	
Minutes of the Senior Management Team and other internal administrative bodies .....	
Reports made by the head teacher or the management team .....	
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities .....	
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities .....	
Professional development plans .....	
School development plans.....	
Admissions- if the admission is successful .....	
Admissions- if the appeal is unsuccessful.....	
Admissions- Secondary Schools Casual.....	
Supplementary information form including additional information such as religion, medical conditions etc .....	
PUPILS .....	
Admission Registers .....	

Attendance registers .....	
Pupil files retained in schools.....	
Pupil files .....	
Special Educational Needs files, reviews and Individual Education Plans.....	
Correspondence Relating to Authorised Absence and Issues .....	
Examination results .....	
Any other records created in the course of contact with pupils.....	
Statement maintained under The Education Act 1996 - Section 324 .....	
Proposed statement or amended statement .....	
Advice and information to parents regarding educational needs .....	
Accessibility Strategy .....	
Parental permission slips for school trips - where there has been no major incident.....	
Parental permission slips for school trips - where there has been a major incident .....	
Records created by schools to obtain approval to run an Educational Visit outside the Classroom	
- Primary Schools.....	
Records created by schools to obtain approval to run an Educational Visit outside the Classroom	
- Secondary Schools .....	
Walking Bus registers .....	
<b>CURRICULUM .....</b>	<b>8</b>
School Development Plan .....	
Curriculum returns.....	
Schemes of work.....	
Timetable .....	
Class record books.....	
Mark Books .....	
Record of homework set .....	
Pupils' work .....	
Examination results .....	
SATS records - Examination Papers and Results .....	
PAN reports .....	
Value Added & Contextual Data .....	
Self Evaluation forms .....	
<b>PERSONNEL FILES HELD IN SCHOOL.....</b>	<b>10</b>
Timesheets, sick pay .....	
Staff Personal files .....	
Interview notes and recruitment records .....	
Pre-employment vetting information (including DBS checks) .....	
Disciplinary proceedings .....	
Records relating to accident / injury at work .....	
Annual appraisal / assessment records .....	
Salary cards .....	

Maternity pay records .....	
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 .....	
Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure.....	
<b>HEALTH &amp; SAFETY .....</b>	<b>12</b>
Accessibility Plans.....	
Accident Reporting .....	
Adults .....	
Children .....	
COSHH .....	
Incident reports.....	
Policy Statements .....	
Risk Assessments .....	
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos .....	
Process of monitoring of areas where employees and persons are likely to have come in contact with radiation.....	
Fire Precautions log books.....	
<b>ADMINISITIVE.....</b>	<b>13</b>
Employer's Liability certificate .....	
Inventories of equipment & furniture .....	
General file series .....	
School brochure or prospectus.....	
Circulars (staff/parents/pupils) .....	
Newsletters, ephemera .....	
Visitors book .....	
PTA/Old Pupils Associations .....	
<b>FINANCE.....</b>	<b>14</b>
Annual Accounts .....	
Loans and grants.....	
Contracts .....	
Budget reports, budget monitoring etc .....	
Invoice, receipts and other records covered by the Financial Regulations.....	
Annual Budget and background papers .....	
Order books and requisitions .....	
Delivery Documentation .....	
Debtors' Records.....	
School Fund - Cheque books.....	
School Fund - Paying in books.....	
School Fund - Ledger .....	
School Fund - Invoices .....	
School Fund - Receipts.....	



School Fund - Bank statements .....	
School Fund - School Journey books .....	
Student grant applications.....	
Free school meals registers .....	
Petty cash books .....	
<b>PROPERTY.....</b>	<b>16</b>
Title Deeds .....	
Plans .....	
Maintenance and contractors .....	
Leases .....	
Lettings .....	
Burglary, theft and vandalism report forms .....	
Maintenance log books.....	
Contractors' Reports .....	
<b>LOCAL AUTHORITY .....</b>	<b>16</b>
Secondary transfer sheets (Primary) .....	
Attendance returns .....	
Circulars from LEA .....	
<b>DEPARTMENT FOR CHILDREN, SCHOOLS &amp; FAMILIES.....</b>	<b>16</b>
HMI reports.....	

OFSTED reports and papers.....	
Returns .....	
Circulars from Department for Children, Schools and Families .....	
CONNEXIONS .....	
Service level agreements.....	
Work Experience agreement .....	
SCHOOL MEALS .....	
Dinner Register.....	
School Meals Summary Sheets .....	
FAMILY LIAISON OFFICERS & HOME SCHOOL LIAISON ASSISTANTS .....	
Day Books .....	
Reports for outside agencies - where the report has been included on the case file created by the outside agency .....	
Referral forms .....	
Contact data sheets .....	
Contact database entries .....	
Group Registers .....	
Template for Destruction log.....	
Confidential Waste Disposal .....	
WHAT HAPPENS TO YOUR COMPUTER EQUIPMENT? .....	
WHAT IS THE PROCESS.....	
WHAT HAPPENS TO THE WORKING EQUIPMENT? .....	
WHAT HAPPENS TO THE NON WORKING OR VERY LOW VALUE EQUIPMENT? .....	
WHAT HAPPENS THEN? .....	
WHY SHOULD WE RECYCLE? .....	
LEWISHAM SCHOOLS IT RECYCLING COLLECTIONS .....	

## 2 RM Register

### **Records Management- Retention Guidelines for Schools**

version 4 May 2012

#### **2.1 CHILD PROTECTION**

<b>Doc Ref</b>	<b>Basic file description</b>	<b>Data Protection</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative</b>
1.1	Child protection files	yes	Education Act 2002, s175, RELATED GUIDANCE 'Safeguarding Children in Education' September 2004	DOB + 25 years	SECURE DISPOSAL
1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff " November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL

#### **GOVERNORS**

<b>Doc Ref</b>	<b>Basic file description</b>	<b>Data Protection</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative</b>
2.1	<b>Minutes</b>				
	Principal set (signed)	no		Permanent	Retain in school for 6 years from date of meeting

	Inspection copy	no		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they should be shredded]
2.2	Agendas	no		Date of meeting	SECURE DISPOSAL
2.3	Reports	no		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.4	Annual parent meeting papers	no		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.5	Instruments of Government	no		Permanent	Retain in school whilst school is open
2.6	Trusts and Endowments	no		Permanent	Retain in school whilst operationally required
2.7	Action Plans	no		Date of action plan + 3 years	SECURE DISPOSAL
2.8	Policy documents	no		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)
2.9	Complaint files	no			
2.10	Annual Reports required by the Department for Education	no	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	
2.11	Proposals for schools to become, or be established as Specialist Status schools	no		Current year + 3 years	

## MANAGEMENT

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operations)	Action at the end of the administrative life of record
3.1	Log books	yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry
3.2	Minutes of the Senior Management Team and other internal administrative bodies	yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting
3.3	Reports made by the head teacher or the management team	yes		Date of meeting + 3 years	Retain in the school for 3 years from meeting
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	yes		Closure of file + 6 years	SECURE DISPOSAL
3.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	no		Date of correspondence + 3 years	SECURE DISPOSAL
3.6	Professional development plans	yes		Closure + 6 years	SECURE DISPOSAL
3.7	School development plans	yes		Closure + 6 years	review
3.8	Admissions- if the admission is successful	yes		Admission + 1 year	SECURE DISPOSAL

3.9	Admissions- if the appeal is unsuccessful	yes		Resolution of case + 1 year	SECURE DISPOSAL
3.10	Admissions- Secondary Schools Casual	yes		current year + 1 year	SECURE DISPOSAL
3.11		yes		current year + year	SECURE DISPOSAL
3.12	Supplementary information form including additional information such as religion, medical conditions etc.				

## PUPILS

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
4.1	Admission Registers	yes		Date of last entry in the book (or le) + 6 years Re consider Retention Period. Feedback from Teaching Relative was thought to be 7 Year Retention. These records are no longer generated in paper but electronically held using SIMS BROCON software.	Retain in the school for 6 years from the date of the last entry then consider transfer to the Archives

4.2	Attendance registers	yes		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]
<b>4.3</b>	<b>Pupil files retained in schools</b>	<b>yes</b>			
4.3a	Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Pupil Referral Unit
4.3b	Secondary		Limitation Act 1980	DOB of the pupil + 25 years	SECURE DISPOSAL
<b>4.4</b>	<b>Pupil files</b>	<b>yes</b>			
4.4a	Primary			Retain for the time which the pupil remains at the primary school	SECURE DISPOSAL
4.4b	Secondary			DOB of the pupil + 25 years	SECURE DISPOSAL

4.5	Special Educational Needs files, reviews and Individual Education Plans	yes		<p>DOB of the pupil + 25 years the review</p> <p>NOTE: This retention period is the minimum period that any pupil le should be kept. Some authorities choose to keep SEN les for a longer period of time to defend themselves in a “failure to provide a sufficient education” case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.</p>	SECURE DISPOSAL
4.6	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL
<b>4.7</b>	<b>Examination results</b>	<b>Yes</b>			
4.7a	Public	No		Year of examinations + 6 years	SECURE DISPOSAL
4.7b	Internal examination results	Yes		Current year + 5 years 5	SECURE DISPOSAL



4.8	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL
4.9	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
4.11	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.12	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.13	Parental permission slips for school trips - where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
4.14	Parental permission slips for school trips - where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL

4.15	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	No	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 14 years 6	N
4.16	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	No	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	N
4.17	Walking Bus registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

## 2.2 CURRICULUM

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
5.1	School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL

5.3	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.4	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.5	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.6	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.8	Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.9	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL

5.10	SATS records - Examination Papers and Results	Yes		Current year + 6 years	SECURE DISPOSAL
5.11	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
5.12	Value Added & Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
5.13	Self Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

## 2.3 PERSONNEL FILES HELD IN SCHOOL

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
6.2	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL
6.4	Pre-employment vetting information (including DBS checks)	No	DBS guidelines	Date of check + 6 months	SECURE DISPOSAL (by the designated member of staff)
6.5	Disciplinary proceedings	Yes	Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.		
6.5a	oral warning			Date of warning + 6 months	SECURE DISPOSAL If this is placed on a personal file it must be weeded from the file.
6.5b	written warning - level one			Date of warning + 6 months	SECURE DISPOSAL

6.5c	written warning - level two			Date of warning + 12 months	SECURE DISPOSAL
6.5d	final warning			Date of warning + 18 months	SECURE DISPOSAL
6.5e	case not found			If child protection related please see 1.2 otherwise SECURE DISPOSAL immediately at the conclusion of the case	SECURE DISPOSAL
6.6	Records relating to accident / injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
6.7	Annual appraisal / assessment records	No		Current year + 5 years	SECURE DISPOSAL
6.8	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year +3yrs	SECURE DISPOSAL
6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

6.11	Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file.	
------	--	-----	--	--	--

## 2.4 HEALTH & SAFETY

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
7.1	Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.2a	Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
7.2b	Children	Yes		DOB of child + 25 years 8 (A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.)	SECURE DISPOSAL

7.3	COSHH			Current year + 10 years [where appropriate an additional retention period may be allocated]	
7.4	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL
7.5	Policy Statements			Date of expiry + 1 year	SECURE DISPOSAL
7.6	Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SECURE DISPOSAL
7.9	Fire Precautions log books			Current year + 6 years	SECURE DISPOSAL

## 2.5 ADMINISITIVE

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
8.1	Employer's Liability certificate			Closure of the school + 40 years	SECURE DISPOSAL
8.2	Inventories of equipment & furniture			Current year + 6 years	SECURE DISPOSAL
8.3	General file series			Current year + 5 years	Review to see whether a further retention period is required

8.4	School brochure or prospectus			Current year + 3 years	
8.5	Circulars (staff/parents/pupils)			Current year + 1 year	SECURE DISPOSAL
8.6	Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required
8.7	Visitors book			Current year + 2 years	Review to see whether a further retention period is required
8.8	PTA/Old Pupils Associations			Current year + 6 years	Review to see whether a further retention period is required

## 2.6 FINANCE

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
9.1	Annual Accounts		Financial Regulations	Current year + 6 years	
9.2	Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
<b>9.3</b>	<b>Contracts</b>				
9.3a	under seal			Contract completion date + 12 years	SECURE DISPOSAL
9.3b	under signature			Contract completion date + 6 years	SECURE DISPOSAL
9.3c	monitoring records			Current year + 2 years	SECURE DISPOSAL
9.4	Copy orders			Current year + 2 years	SECURE DISPOSAL
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	SECURE DISPOSAL



9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
9.7	Annual Budget and background papers			Current year + 6 years	SECURE DISPOSAL
9.8	Order books and requisitions			Current year + 6 years	SECURE DISPOSAL
9.9	Delivery Documentation			Current year + 6 years	SECURE DISPOSAL
9.10	Debtors' Records		Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
9.11	School Fund - Cheque books			Current year + 3 years	SECURE DISPOSAL
9.12	School Fund - Paying in books			Current year + 6 years then review	SECURE DISPOSAL
9.13	School Fund - Ledger			Current year + 6 years then review	SECURE DISPOSAL
9.14	School Fund - Invoices			Current year + 6 years then review	SECURE DISPOSAL
9.15	School Fund - Receipts			Current year + 6 years	SECURE DISPOSAL
9.16	School Fund - Bank statements			Current year + 6 years then review	SECURE DISPOSAL
9.17	School Fund - School Journey books			Current year + 6 years then review	SECURE DISPOSAL
9.18	Student grant applications			Current year + 3 years	SECURE DISPOSAL
9.19	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
9.20	Petty cash books			Current year + 6 years	SECURE DISPOSAL

## 2.7 PROPERTY

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
10.1	Title Deeds			Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
10.2	Plans			Permanent	Retain in school whilst operational
10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
10.4	Leases			Expiry of lease + 6 years	SECURE DISPOSAL
10.5	Lettings			Current year + 3 years	SECURE DISPOSAL
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
10.7	Maintenance log books			Current year + 6 years	SECURE DISPOSAL
10.8	Contractors' Reports			Current year + 6 years	SECURE DISPOSAL

## 2.8 LOCAL AUTHORITY

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
11.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
11.3	Circulars from LEA			Whilst required operationally	Review to see whether a further retention period is required

## 2.9 DEPARTMENT FOR CHILDREN, SCHOOLS & FAMILIES

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
12.1	HMI reports			These do not need to be kept any longer	

12.2	OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required
12.3	Returns			Current year + 6 years	SECURE DISPOSAL
12.4	Circulars from Department for Children, Schools and Families			Whilst operationally required	Review to see whether a further retention period is required

## CONNEXIONS

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
13.1	Service level agreements			Until superseded	SECURE DISPOSAL
13.2	Work Experience agreement			DOB of child + 18 years	SECURE DISPOSAL

## SCHOOL MEALS

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
14.1	Dinner Register			Current year + 3 years	SECURE DISPOSAL
14.2	School Meals Summary Sheets			Current year + 3 years	SECURE DISPOSAL

## FAMILY LIAISON OFFICERS & HOME SCHOOL LIAISON ASSISTANTS

Doc Ref	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of record
15.1	Day Books	Yes		Current year + 2 years then review	SECURE DISPOSAL
15.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL
15.3	Referral forms	Yes		While the referral is current	SECURE DISPOSAL

15.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
15.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	DELETE
15.6	Group Registers	Yes		Current year + 2 years	SECURE DISPOSAL

## Template for Destruction log

[illegible]

## General

- It is essential that any paper records you destroy, which contain confidential, 'personal' or 'sensitive' information, are either shredded or destroyed via the confidential waste service.
- If you are unsure of the legal, administrative or archival retention requirements for particular information please contact The Corporate Information Team for advice.
- Most confidential material is subject to the Data Protection Act. Under the Act the individual handling or processing confidential data is personally responsible for the proper disposal of such data.

### 3 Confidential Waste Disposal



If you require confidential waste bin/s on a regular basis or for a one-off situation, please contact Lewisham Property Services, who will provide you with all available options and costs.

#### 3.1.1 Contacts:

**Barbara Hussey (Cleaning & Security Contract Officer)** Email: [Barbara.hussey@lewisham.gov.uk](mailto:Barbara.hussey@lewisham.gov.uk)  
Tel: 0208-314-666

**Or**  
**Andree Browne (Operations Manager)**  
Email: [Andre.browne@lewisham.gov.uk](mailto:Andre.browne@lewisham.gov.uk) Tel: 0208-314-7978

## **4 IT equipment and Premises equipment**

An inventory of all items with a value over £100 (items of a lower value can be added to the inventory if deemed appropriate) will be maintained. Items should be asset marked and also have the school name clearly marked. The inventory should list the date of purchase, the value, description, the serial number and the location.

Staff should inform the Premises teams (for premeised equipmemnt) / IT teams (for IT equipment) if any equipment is purchased that needs to be added to the inventory.

All equipment of an attractive and portable nature should be visibly security marked to deter potential thieves.

The Headteacher will ensure that a check of all items to the inventory is carried out each year and, following this, certify the inventory book by signing and dating the record. Any missing items should be noted and promptly investigated. Written records of investigations carried out for any missing items should be held with the inventory records.

Any damaged, surplus or out-dated items should be considered for disposal. Written records of obsolete or redundant items, including their value, repair or replacement costs, should be held with the inventory records. The records should be signed by the Headteacher and reported to the Executive Head.

The IT / Premises team must record all items on the Write Off register "destruction of Records Spreadsheet" (attached to this policy) which is held by the IT manager and Premises Officer in each school along with the Asset registers.

The following detail must be recorded:

- Description of the equipment (all items listed seperatly)
- Quantity of records
- Method of destruction
- Date of destruction
- Authorised staff name (will be IT or Premises)
- Aprooved by will be School Business Manager/ Head teacher

One the items have been approved for write off the Premises / It team must contact a reputable company to collect and dispose of the equipment.

Companies that can be used:

ICT: ICEX or CDL

PREMISES: Romulus Dringa – Upper teir waste carrier and dealer

IT

These companies specialise in the management and disposal of redundant IT assets, providing a secure and highly accredited service. Any company used must be an accredited member of ADISA (Asset Disposal & Information Security Alliance).

All IT equipment must hard drive wiped before collection or certification that it is destroyed on collection.

A copy of the certificate must be provided to the IT manager to state it has been wiped / destroyed.

**ICEX Ltd Head Office**, Europa Park, Croft Way Witham, Essex CM8 2FN, T: 01376 503 900, E: [info@icex.co.uk](mailto:info@icex.co.uk)

**CDL House, Davy Road, Runcorn, Cheshire, WA7 1PZ.** T: [0333 060 9531](tel:03330609531) E: [sales@computerdisposals.com](mailto:sales@computerdisposals.com)

All certificates must be kept with the write of register

## **ICEX / CDL PROCESS**

ICEX / CDL will send CRB checked staff that will arrive in secure, GPS tracked vehicles. All assets are physically counted and are given their own individual, unique barcode at the point of collection.

A Consignment Note – Transfer of Duty of Care – is provided prior to assets being removed from site. All assets are logged on arrival at their facility.

Any asset bearing data is erased using CESG approved software. Certification of the process is provided.

In the event a hard drive cannot be erased, it is removed, logged and shredded within our own facility. Certification of the process is provided.

All assets are cleaned; asset tags or identifying marks are removed. An audit of all internal components is carried out.

A comprehensive inventory is produced as a record of what has been recycled.

### **Premises**

This company specialises in the removal of any assets. Any company used must be an accredited member and hold a certificate of Registration under the waste regulation 2011

The premises manager / officer must ensure they have seen the certificate before collection.

A copy of the certificate must be kept with the write of register (destruction of records spreadsheet).

## **Destruction of Records**



[illegible]