



Burlington Junior School

Records Management Policy

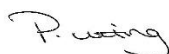
Written By	Senior Staff, School Office team
Frequency of Review	4 years
Date reviewed and approved by Governing Body	May 2021
Date of next review	May 2025
Display on Website	✓
Purpose	Burlington Junior School is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible to the appropriate individuals. In line with the requirements of the GDPR, the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.
Consultation	Governors ✓
	Parents x
	Pupils x
	Staff ✓
Links with other policies	Safeguarding Policy GDPR/data protection Policy Privacy Policy

Statement of intent

Burlington Junior School is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible to the appropriate individuals. In line with the requirements of the GDPR, the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, retained and disposed of to meet the school's statutory requirements.

This document complies with the requirements set out in the GDPR and Data Protection Act 2018.



Signed by:

Headteacher _____

Date: May 2021

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:

- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- Data Protection Act 2018

1.2. This policy also has due regard to the following guidance:

- Information Records Management Society (IRMS) (2019) 'Information Management Toolkit for Schools'
- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2018) 'Careers guidance and access for education and training providers'

2. Responsibilities

- 2.1. The whole school has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.
- 2.2. The headteacher holds the overall responsibility for this policy and for ensuring it is implemented correctly.
- 2.3. The SBM is responsible for the management of records at the school.
- 2.4. The SBM is responsible for promoting compliance with this policy and reviewing the policy every 4 years, in conjunction with the headteacher.
- 2.5. The SBM is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of safely and correctly.
- 2.6. All staff members are responsible for ensuring that any records they are responsible for (including emails) are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of pupil records

- 3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievements.
- 3.2. The following information is stored on the front of a pupil record, and will be easily accessible:
 - Forename, surname, and date of birth
 - Unique pupil number
 - Note of the date when the file was opened
- 3.3. The following information is stored electronically.
 - Any preferred names
 - Emergency contact details and the name of the pupil's doctor
 - Any allergies or other medical conditions that are important to be aware of
 - Names of people with parental responsibility, including their home address(es) and telephone number(s)
 - Any other agency involvement, e.g. speech and language therapist
 - Reference to any other linked files
- 3.4. The following information is stored electronically, and will be easily accessible:
 - Admissions form
 - Details of any SEND
 - If the pupil has attended an early years setting, the record of transfer
 - Data collection or data checking form
 - Annual written reports to parents
 - Notes relating to major incidents and accidents involving the pupil
 - Any information about an EHC plan and support offered in relation to the EHC plan
 - Medical information relevant to the pupil's on-going education and behaviour
 - Any notes indicating child protection disclosures and reports
 - Any information relating to exclusions
 - Any correspondence with parents or external agencies relating to major issues, e.g. mental health
 - Notes indicating that records of complaints made by parents or the pupil

- 3.5. The following information is subject to shorter retention periods and, therefore, will be stored separately in appropriately named files which are kept in the school office:
- Attendance registers and information
 - Absence notes and correspondence
 - Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
 - Accident forms – forms about major accidents will be recorded on the pupil record
 - Consent to administer medication and administration records
 - Correspondence with parents about minor issues, e.g. behaviour
- 3.6. Hard copies of disclosures and reports relating to child protection are stored in a securely locked filing cabinet by the Designated Safeguarding Officer.
- 3.7. Hard copies of complaints made by parents or pupils are stored in the pupil's file in the office.
- 3.8. Actual copies of accident and incident information are stored separately on the school's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.
- 3.9. The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.
- 3.10. The school will not keep any copies of information stored within a pupil's record, unless there is ongoing legal action at the time during which the pupil leaves the school. The responsibility for these records will then transfer to the next school that the pupil attends.
- 3.11. The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

4. Retention of records

Description	Why held and what used for	Who holds and who can access	Security controls are in place?	How long is data kept for	Is it duplicated? Where?	Risk category for data
Admissions and pupil reg info (address - child and parent/child dob/telephone number/GP info/SEND/travel info/FSM/ethnicity)	In case of emergency	Information received from Infants or from parents/former school for SEND info. Only accessible to staff via unique login through SIMS	School network managed by Azteq	We can now delete records – keep records for 25 years in the past as no mention of SEN	Paper copies are kept in a locked filing cabinet. School applications are stored by the LA	High risk data but not accessible off-site or shared with outside individuals or organisations (with the exception of SPA and MASH/child protection services through LA.)
Trips and visits permission slips	To ensure pupils are able to go on trips	Admin team	Stored on Tucasi Unique login required	No retention unless there is a major incident (25 years retention)	No	Low
SEND Information	To support children	SENCO, staff on SIMS, parent of pupils	SIMS unique log in required	DOB + 25 years	Yes, in locked filing cabinet	High
Child Protection Information	To protect welfare of child	Locked cabinet, CP access only	Stored in child's file in sealed envelope	Kept in a sealed envelope and retained dob + 25 years & sent onto next school	Not duplicated	high

Description	Why held and what used for	Who holds and who can access	Security controls are in place?	How long is data kept for	Is it duplicated? Where?	Risk category for data
Allegations against a member of staff	To protect welfare of the children	Head teacher and Deputy only SBM – key holder to safe	Sealed envelope signed by HT Only to be opened by HT or Deputy	Until the person's normal retirement age or 10yrs from date of allegation whichever is the longer. NOT to be kept in personnel files if malicious	Locked in safe	High
Health and medical plans	As above	Admin and relevant teaching staff	Kept in child's file	Destroyed when child leaves school or passed onto next school if requested	On SIMS	High
Attendance registers	As above	Admin staff	On SIMS	Three years	No	Medium
Authorised absence	As above	A/A		Current year + 2	No	Low
Academic Information	As above	Available on SIMS	On SIMS	All recorded on SIMS – Once Cygnet IT have sorted package, deletion will take place after 6 years (apart from SEND children) All will be kept as cannot distinguish those who are SEN	No	Medium
Reports	Requirement	All staff	On child's file	Sent to next school	No	High
SATS Information	Requirement	Head/Deputy	Recorded on SIMS	Capita are working on mass deletion	No	High

Description	Why held and what used for	Who holds and who can access	Security controls are in place?	How long is data kept for	Is it duplicated? Where?	Risk category for data
Behaviour Information (Communications/logs/incident forms)	Requirement	Head/Deputy/teaching Staff	Forms kept in file in locked cupboard and copy in child's file Now moved to CPOMS so no need for paper copies since Spring 2021		Child's file Head teacher decides if information is shredded or sent onto senior school	High
Recruitment application forms Successful applicants	To appoint new staff	Eteach/HT/Deputy/SBM/HR (AK)	Locked cabinet in staff files	Length of employment + 6 years	No	High
Unsuccessful applicants		A/A	Locked cabinet	6 months then shredded	No	High
Payroll (Bank account details/NI/Pension details/tax info)	In order to pay staff	SBM/HR Assistant/HT	Locked cabinet	Length of employment + 6 years)	Available on secure portal (EPM)	High
Staff pension		TP & RBK pension website – SBM & HR assistant	Log in required – viewing only	Kept for life at national level		Low
H&S records (accidents)	Safety	Admin staff	Stored in locked cupboard	+ 6 years (adults) 25 years child	No	Medium
Single Central Record	Security for pupils & staff	HR Assistant/ Head/Deputy/SBM	Password protected	Leavers details – name and DBS number only	No	High

Description	Why held and what used for	Who holds and who can access	Security controls are in place?	How long is data kept for	Is it duplicated? Where?	Risk category for data
DBS checks	Not held	On SCR	Number noted, copies NOT stored	Name and Number kept in case of return	No	High
Visitor records	To know who is on site	Office staff	No - anyone can access	Current year + 6 years (stored in loft)	No	Low – just names
Governor meeting minutes	Legal	Clerk	No	6 years	SBM has started keeping paper copies	None – available to view by all
Photos & videos of pupils	NASbox	All staff	NOT to be used unless full agreement from parent	Child's School Life	Only with agreement from parent	High

EPM	Hold payroll/HR info on all staff					
Action HR	RBK DBS application service					
HMRC	Payroll Info	Legal				
DFE	School Census Information	Legal				
SMS	Converts payroll files					
Tucasi	Trip/Lunches reporting					
LGFL	To enrich learning	Children's names only				
Van Cols	Produces child photos for SIMS					
GL assessment	To enrich learning	A/A				
TT Rockstars	To enrich learning	A/A				
Micro librarian	To enrich learning	A/A				
Cygnat	SIMS Data processor					
SAS	Holds teacher absence information					
HCSS	Accounts package for working on payroll costs					
Azteq	IT advisors					

5. Retention of emails

- 5.1. All staff members with an email account will be responsible for managing their inbox.
- 5.2. Emails can act as evidence of the school's activities, i.e. in business and fulfilling statutory duties, so all relevant emails (e.g. invoices) will be retained for at least **12 months**.
- 5.3. Correspondence created by the **SLT** and other members of staff with administrative responsibilities will be retained for **three** years before being reviewed and, if necessary, securely disposed of.
- 5.4. Personal emails, i.e. emails that do not relate to work matters or are from family members, will be deleted as soon as they are no longer needed.
- 5.5. Staff members will not, under any circumstances, create their own email archives, e.g. saving emails on to personal hard drives.
- 5.6. Staff members will be aware that the emails they send could be required to fulfil a SAR or freedom of information (FOI) request. Emails will be drafted carefully, and staff members will review the content before sending.
- 5.7. Individuals, have the right to submit an SAR to gain access to their personal data to verify the lawfulness of the processing – this includes accessing emails.
- 5.8. All SARs will be handled in accordance with the school's **Data Protection Policy**.

6. Identifying information

- 6.1. Under the GDPR, all individuals have the right to data minimisation and data protection by design and default – as the data controller, the school ensures appropriate measures are in place for individuals to exercise this right.
- 6.2. Wherever possible, the school uses pseudonymisation, also known as the 'blurring technique', to reduce the risk of identification.
- 6.3. Where data is required to be retained over time, e.g. attendance data, the school removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

7. Storing and protecting information

- 7.1. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- 7.2. Any room or area where personal or sensitive data is stored will be locked when unattended.
- 7.3. Confidential paper records are not left unattended or in clear view when held in a location with general access.
- 7.4. Personal information is never put in the subject line of an email.
- 7.5. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 7.6. Before sharing data, staff always ensure that:
 - They have consent from data subjects to share it.
 - Adequate security is in place to protect it.
 - The data recipient has been outlined in a privacy notice.
- 7.7. The school has data sharing agreements with all data processors and third parties with whom data is shared.
- 7.8. All staff members implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information is stored in a securely locked filing cabinet, drawer or safe with restricted access.
- 7.9. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- 7.10. The school takes its duties under the GDPR seriously and any unauthorised disclosures may result in disciplinary action.
- 7.11. The **DPO** is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

8. Accessing information

- 8.1. We are transparent with data subjects, the information we hold and how it can be accessed.
- 8.2. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.
- 8.3. The school will adhere to the provisions outlined in the school's **Data Protection Policy** when responding to requests seeking access to personal information.

9. Information audit

- 9.1. The school conducts information audits on an **annual** basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:
 - Paper documents and records
 - Electronic documents and records
 - Databases
 - Video and photographic records
- 9.2. The information audit may be completed in a number of ways, including, but not limited to:
 - Interviews with staff members with key responsibilities – to identify information and information flows, etc.
 - Questionnaires to key staff members to identify information and information flows, etc.
 - A mixture of the above
- 9.3. The **DPO** is responsible for completing the information audit. The information audit will include the following:
 - The school's data needs
 - The information needed to meet those needs
 - The format in which data is stored
 - How long data needs to be kept for
 - Vital records status and any protective marking
 - Who is responsible for maintaining the original document
- 9.4. The **DPO** will consult with staff members involved in the information audit process to ensure that the information is accurate.

- 9.5. Once it has been confirmed that the information is accurate, **the DPO** will record all details on the school's **Data Asset Register**.
- 9.6. The information displayed on the **Data Asset Register** will be shared with the **headteacher** to gain their approval.

10. Monitoring and review

- 10.1. Any changes made to this policy will be communicated to all members of staff and the governing board.