Purley Partnership Federation

Purley Nursery School
Achieving and growing together

Christ Church Primary School
Nurturing lifelong learners with God's guidance

Document Retention Policy

Written April 2018, review date April 2021

Policy Statement

The Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000 states *"Authorities should ensure they keep records they will need for business, regulatory, legal and accountability purposes"*[1] and that *"Authorities should define how long they need to keep particular records, should dispose of them when they are no longer needed and should be able to explain why records are no longer held"*[2].

The Schools recognise that by efficiently managing their records, they will be able to comply with the legal and regulatory obligations and to contribute to the effective overall management of the institutions. Records provide evidence for protecting the legal rights and interests of the schools, and provide evidence for demonstrating performance and accountability.

This document provides the policy framework through which this effective management can be achieved and audited. It has been developed by referring to similar policies held by other schools and with reference to Croydon Council's Records Retention Policy and the GDPR regulations that come into effect from the 25th May 2018.

Purpose

1. Ensure records are held for the correct length of time to meet legislative, regulatory, financial and administrative requirements.
2. Ensure all records, in all mediums, have a retention period applied at point of creation, which is reviewed throughout the records lifecycle, and is checked prior to disposal of the record to ensure current compliance.
3. Ensure records are managed and processed securely, fairly and lawfully throughout the records lifecycle, according to their sensitivity, access and retention requirements.
4. Ensure that records are used for specific and relevant purposes
5. Ensure that they are accurate and kept up to date
6. Ensure records are timely and securely disposed of once use is concluded.
7. Prevent premature destruction of records.
8. Reduce unnecessary duplication.

---

[1] Lord Chancellor's Code of Practice on the management of records, 8 – Keeping records to meet corporate requirements – p.14

[2] Lord Chancellor's Code of Practice on the management of records, 12 Disposal of records – p.20

9. Reduce retention of ephemeral material.
10. Support decision-making and service delivery.
11. Ensure records with corporate or historical value are identified and retained as an archive.

Scope of the policy

1. This policy applies to all records created, received or maintained by staff of the schools in the course of carrying out its functions.
2. Records are defined as all those documents which facilitate the business carried out by the schools and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically.
3. A small percentage of the schools records may be selected for permanent preservation as part of the schools archives or historical research. This should only be done in liaison with the local authority archives centre.

Retention Governance

Retention periods are governed by legislation, regulation, financial requirements and business need. Records should be retained for as long as they are needed and should be destroyed as soon as they cease to be required, thus minimising the costs associated with their maintenance and storage and ensuring retention compliance. Retention periods are fluid, governed by changes to legislation or business need. Therefore, their current accuracy and relevance should be reviewed before application and destruction of records.

There is minimal specific legislation stipulating mandatory retention periods within local government. The majority of retention is determined by risk analysis and business need, defined by common practice, industry standards and guidelines produced by The National Archives (TNA) and the Information and Records Management Society of Great Britain (IRMS). The IRMS has produced the Local Government Classification and Retention Scheme (LGCRS), which is the industry standard for retention governance within local government. Other factors to be considered, where there is no statutory retention requirement, include cost of storage, access requirements and appropriate storage format.

During the course of normal business, many documents are created that after a short period of time serve no purpose and thus become ephemeral. It is therefore essential all records have a retention period applied, which is realistic and which is periodically reviewed, thus ensuring the unnecessary retention of records that have no long-term business need or value once their use is concluded.

ISO 15489-1 states records should be retained that:

- Meet current and future business needs
- Evidence and record past and present decisions
- Are authentic and reliable
- Have integrity and accountability by retaining the context of the record, even where the records systems in which they are retained have undergone significant changes
- Are destroyed in an authorised and systematic manner once their use and retention has been concluded.

Responsibilities

1. The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. In light of the new Data Protection Regulations from May 25th 2018, the schools have to appointed a DPO (Data Protection Officer) to monitor all the records within the school. This person will be the Deputy Head Teacher from Christ Church School and the Lead Teacher from Purley Nursery School. The person with overall responsibility for this policy is the Executive Head Teacher.
2. The DPO for each school will give guidance about good records management practice and will promote compliance with this policy so that information can be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

3. Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the schools records management guidelines.

Relationship with existing policies

This policy has been drawn up within the context of the Data Protection and Freedom of Information Policy and with other legislation or regulations (including audit and equal opportunities) affecting the school

Disposal of Records

1. Records should be routinely identified at the end of the designated retention period and a decision made as to whether destruction is relevant, based on current retention requirements and business need. See below for retention guidelines.
2. Destruction of records should be authorised by a person designated with responsibility, i.e. a senior officer.
3. Records authorised for destruction should be confidentially shredded and documented to ensure accountability and to provide an audit trail. See each school's Data Deletion/Disposal Record for the evidence of document deletion.
4. Records which are subject to a current Freedom of Information or Data Protection request, an investigation or public enquiry must not be destroyed.

Reporting a Breach

A data breach could be:

- The (accidental) destruction of data
- Loss or theft of items/devices storing data
- The (accidental) alteration of the data – human error
- Unauthorised disclosure of or access to personal data
- Hacking
- Data obtained by deception
- Unforeseen circumstances – fire, flood etc.

Staff in both schools will have regular training and updates on how to report a data breach by completing a Data Protection Breach form (Appendix 1) and handing it to the DPO. The DPO for each school is responsible for logging the breach and deciding whether it requires reporting to the ICO (Information Commissioner's Office) within 72hours. The DPO will decide if the breach has successfully been contained and risk assessed for future or if it requires reporting to the ICO. All breaches, regardless of if reported to the ICO or not, are to be logged on the Data Protection Breach Log.

Retention Guidelines Summary Table

(Only those records where there may be a data protection issue are listed)

Basic File Description	Data Protection Issue	Retention Period	Action at end of admin life of record
Child Protection Files	Yes	Retain for time pupil in school	Transfer to new school
		If destination is unknown this is DOB +25 years.	Secure disposal
Electronic pupil files	Yes	2 years after the child has left the school (unless destination unknown then it is DOB +25 years)	Secure deletion
Child Photos were parental permission has been given and not withdrawn	Yes	2 years after the child has left the school	Secure disposal
Photos of children or their learning on the iPads	Yes	Termly remote wiping of iPads	Secure deletion
Staff Personal Files	Yes	Termination + 15 years	Secure disposal
Annual appraisal/assessment records	Yes	Current year + 5 years	Secure disposal
Health & Safety -Adults	Yes	Date of incident +7 years	Secure disposal
Records relating to injury at work	Yes	Date of injury + 12 years	Secure disposal
Health & Safety -Children	Yes	DOB +25 years	Secure disposal
Incident reports	Yes	Current year + 20 years	Secure disposal
Risk Assessments	Yes	Current year + 2 years	Secure disposal
Finance	Yes	Current year + 6 years	Secure disposal
Pupil Files (Primary) including SEND files	Yes	Retain for time pupil in school	Transfer to new school
Electronic files or information on children (e.g. SEND and planning/groupings) on the school network	Yes	2 years after the child has left the school	Secure deletion
Parental permission slips trips – Major incident occurred	Yes	DOB of pupil involved + 25 years All slips to be retained	Secure disposal
Recruitment application information – unsuccessful candidates	Yes	1 year after the post has been filled	Secure disposal
Complaints requiring the involvement the governing body	Yes	6 years after resolution	Secure disposal
Insurance claims against the school	Yes	2 years after the case is closed	Secure disposal
Governing body and committee signed minutes	No	7 years	Disposal
SIMS and Target Tracker	Yes	2 years after the child has left the school	Secure deletion
Website information/photos	Yes	Photos on the website kept no longer than 2 years after the child has left the school	Secure deletion

Staff emails	Yes	2 years automatic deletion of emails	Automatic secure deletion
Other computer software or apps where data is stored that allows the individual to be recognised	Yes	2 years after the child has left the school	Secure deletion
CCTV	Yes	3months	Secure deletion

Appendix 1

Data Protection Breach Form

Name of person reporting breach: _____

Date: _____

Name of person responsible for the breach (if known): _____

Category of Breach (please tick):

Type of breach	**Tick**
(Accidental) destruction of data	
Loss or theft of items/devices storing data	
(Accidental) alteration of the data – human error	
Unauthorised disclosure of or access to personal data	
Hacking	
Data obtained by deception	
Unforeseen circumstances – fire, flood etc	
Other (please state)	

Please provide more details about the breach (how and when, what data was involved, steps taken already):

Action taken, when and by whom (including details on containment/recovery, assessing on-going risk, notification, evaluation):

DPO – Stephanie Wright