Charlton Kings Infants' School

Data Retention Policy

Governor Committee Responsible:	Finance and Operations	Governor Lead:	Alan Waller Alan.Waller@ckis.org.uk
Status	Non-Statutory	Review Cycle	Bi-Annual
Last Review	1.06.2019	Next Review Date	June 2021

Designation	Name	Date	Signature
Chair of Governors	Henning Schmidt	12.06.19	
Head Teacher	Katie James	12.06.19	

Introduction

The purpose of this policy is to set out the general principles for retention of data and give specific guidelines for different types of data.

General principles

The Data Protection Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

This is the fifth data protection principle set out in the Act and, in practice, it means that it is necessary to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under both the Data Protection Act 1998 and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored. This schedule is Appendix 1 to this policy.

Information to individuals about the deletion of data

The ICO's Personal Information online code of practice says:

"It is good practice to make it clear to people what will happen to their information when they close their account – i.e. if it will be deleted irretrievably or simply deactivated or archived. Remember that if you do archive personal data, the rules of data protection, including subject access rights, still apply to it.

If you offer users the option to delete personally identifiable information uploaded by them, the deletion must be real i.e. the content should not be recoverable in any way, for example, by accessing a URL from that site. It is bad practice to give a user the impression that a deletion is absolute, when in fact it is not."

Deletion of data

At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful where many records of the same type are held.

However, there is a significant difference between permanently deleting a record and archiving it. If a record is archived or stored offline, this should reduce its availability and the risk of misuse or mistake. However, you should only archive a record (rather than delete it) if you still need to hold it. You must be prepared to give subject access to it, and to comply with the data protection principles. If it is appropriate to delete a record from a live system, it should also be deleted from any back-up of the information on that system.

The word 'deletion' can mean different things in relation to electronic data. We have produced detailed guidance which sets out how organisations can ensure compliance with the DPA, in particular the fifth data protection principle, when archiving or deleting personal information:

The DPA does not define 'delete' or 'deletion' – but a plain English interpretation implies 'destruction'. With paper records it is relatively easy to say whether information had been deleted or not, for example through incineration. The situation can be less certain with electronic storage, where information that has been 'deleted' may still exist, in some form or another, within the school's systems.

The Information Commissioner's Office seeks to provide clarification of the difference between archiving and deletion and sets out the following guidance:

There is a significant difference between deleting information irretrievably, archiving it in a structured, retrievable manner or retaining it as random data in an un-emptied electronic wastebasket. Information that is archived, for example, is subject to the same data protection rules as 'live' information, although information that is in effect inert is far less likely to have any unfair or detrimental effect on an individual than live information. However, the ICO will adopt a realistic approach in terms of recognising that deleting information from a system is not always a straightforward matter and that it is possible to put information 'beyond use', and for data protection compliance issues to be 'suspended' provided certain safeguards are in place:

- *Information has been deleted with no intention on the part of the data controller to use or access this again, but which may still exist in the electronic ether. For example, it could be waiting to be over-written with other data*
- *Information that should have been deleted but is in fact still held on a live system because, for technical reasons, it is not possible to delete this information without also deleting other information held in the same batch.*

The ICO will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the data controller holding it:

- *Is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;*

- *does not give any other organisation access to the personal data;*
- *surrounds the personal data with appropriate technical and organisational security; and*
- *commits to permanent deletion of the information if, or when, this becomes possible.*

Data Controllers will not be required to grant individuals subject access to the personal data provided that all four safeguards above are in place. Nor will we take any action over compliance with the fifth data protection principle. The Data Controller in Charlton Kings Infants' School is the School Business Manager.

Appendix 1

Please refer to the IRMS Information Management Toolkit for Schools.