



Data Management

Standens Barn Primary School

General Data Protection Regulations Audit

Ruth Hawker

Company Director

BSc (Hons), MBA, MSc HRM (Open), CMIOSH, SIIRSM, FCMI, Chartered FCIPD

Becky Clark

Director

MAAT, Cert ISOH, MInstLM, AIIRSM

Molly O'Donnell

Assistant Director

BA (Hons), HND



Contents

- 1.0 Overall Summary 3
 - 1.1 Date of Audit and Key Information3
 - 1.2 Summary of the Audit3
- 2.0 School Details 4
- 3.0 Explanation of the Audit 5
 - 3.1 Audit Purpose5
 - 3.2 Audit Remit5
 - 3.3 Audit Owner5
 - 3.4 Audit Distribution.....5
 - 3.5 Audit Review Schedule5
- 4.0 Audit Process 6
- Main Report and Evidence 7
 - 4.1 School Audit Table..... **Error! Bookmark not defined.**
- 5.0 Appendix **Error! Bookmark not defined.**
 - 5.1 Listings of documentary evidence..... **Error! Bookmark not defined.**
 - 5.2 Listings of observations **Error! Bookmark not defined.**
 - 5.3 Listings of interviews..... **Error! Bookmark not defined.**



1.0 Overall Summary

1.1 Date of Audit and Key Information

Date	18 th March 2025
Auditor	Becky Clark

1.2 Summary of the Audit

A data protection audit is a way of finding out if data management is taking place in line with the standards required by the General Data Protection Regulations. It lets organisations know where suitable and sufficient controls are in place, where improvements are required and areas of non-compliance.

The aim is; to allow quality improvement in systems and processes to reduce the likelihood of a data breach involving personal identifiable information; to ensure that in the event of a breach the organization can show that it has taken appropriate practical steps outlined as necessary by the Information Commissioners Office.



2.0 School Details

School Name	Standens Barn Primary School
School Address	Flaxwell Court, Northampton, NN3 9EH
Telephone Number	01604 413151
Headteacher	Mrs Amie James
Chair of Governors / Trustees	Ms Pauline Matheson-Marks
Type of School	Primary
School Category	Academy
Age Range of Pupils	4-11
Number of Pupils on Roll	372



3.0 Explanation of the Audit

This audit does not supersede existing procedures or arrangements associated with GDPR.

3.1 Audit Purpose

The audit provides an assessment of whether your organisation is following good data protection practice. The audit plays a key role in assisting organisations in understanding and meeting their data protection obligations. The audit looks at whether you have effective controls in place alongside fit for purpose policies and procedures to support your data protection obligations. We check if you are following data protection legislation as it applies to your organisation and will report with recommendations on how to improve.

3.2 Audit Remit

The audit must be perceived as a positive management tool for the employer. It should have unrestricted access to both external and internal auditors, keeping cost-effectiveness, independence and objectivity under review.

The audit will ensure the undertaking of the employer's responsibilities outlined in section 1.1.

3.3 Audit Owner

The Headteacher is the owner of the audit and is responsible for its distribution and action. The Governors have the responsibility to consider and act upon the findings in accordance with the General Data Protection policy and other related school policies.

3.4 Audit Distribution

The audit will be distributed to staff (teachers and support staff) and governors if applicable. New staff and governors will be informed of the actions of the audit during their induction as a positive management communication tool to embed the importance of GDPR into the schools culture.

3.5 Audit Review Schedule

The audit will be conducted on an annual basis, unless the audit has been activated or changes occur which then require a review.



4.0 Audit Process

The audit reflects ICO guidance for leading GDPR at work. It also audits the employer's performance of legal duties placed on the employer under the General Data Protection Regulation which was introduced in May 2018.



Main Report and Evidence

Previous Recommendations	Completed	Observations
Record of Data Breaches Data Breaches will be recorded if and when required	None to date	
What checks are completed to ensure that staff/contractors comply with GDPR? Annual Training for staff, Amey Contractors to be checked	Outstanding	
Has personal information been reduced to an acceptable level? Some classrooms were displaying student computer logins.	Yes	Have been removed
	Compliant	Observations
General		
Who is the Data Protection Lead who oversees data compliance and liaises with the external DPO	Yes	Head Teach – Amie James
Does the school have Data Protection Policy When was it last reviewed?	Yes	Updated in the Summer 2024
Which Privacy Notices do the school hold (Pupil, Workforce, CCTV, Trustees, LAC/CIN others?)	Yes	
Are privacy notices easily accessible? Where are they available?	Yes	Website
Does the school have an Information Audit? When was it last reviewed? Evidence?	Yes	December 2024
Does the school have a retention document that is in line with the information Audit?	Yes	
What system is in place to ensure the school destroy documents in line with the retention document?	Yes	Regularly reviewed.
Does the school record data that is destroyed? How and where?	No	Ensure data destroyed is evidenced
Check – Personnel files to ensure unsuccessful candidates applications have been destroyed after six months	Yes	
Check – Personnel (eg. No DBS Certificates are in personnel files)	Yes	
Check – Year 2 Pupil Files to ensure proof of address has been destroyed	Yes	
Check – Pupil File (eg. No birth certificates are in pupil file)	Yes	
Are parents and employees fully informed of how you use their data? What information do you give parents and employees?	Yes	Signpost parents to website and provide information on the admissions form In application pack for staff
Where CCTV is monitored are there clear procedures in place to inform individuals	Yes	Signage around the school



Personal Data		
What personal data is collected? Is this recorded on the information audit?	Yes	
Check Information Audit		
How is personal data collected, is this recorded on the information audit?	Yes	Admissions pack updated via Arbour. Staff inform directly to the office Reminders are set regularly All information is updated through WAND from Arbour
Check Information Audit		
If online data is collected (Arbour, parent pay etc) What procedures are in place to verify the age of the person online?	Partial	Check on admission, taster day, parents evening.
How does the school verify email accounts of parents/carers?	Partial	Check on admission, taster day, parents evening.
Is there a documented policy/procedure for subject access request	Yes	
Are subject access requests responded to within 30 days?	Yes	
Are procedures in place to provide individuals with their personal data in a structured and readable format?	Yes	
Accuracy and Retentions		
Is personal data only used for the purposes for which it was originally collected?	Yes	
Is the personal data collected limited to what is necessary for the purposes for which it is processed?	Yes	
Are procedures in place to ensure personal data is kept up to date and accurate?	Yes	
Where data needs to be corrected or amended is there a written process in place for the data to be changed?	Yes	Check Policy
Do you have procedures in place to ensure data is destroyed securely?	Yes	Shredder on site and off site shredder
Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records	Yes	
Other Obligations		
Have agreements with suppliers been reviewed	Yes	Trust level
Where data breaches or SAR's occur are there documented procedures in place and are all staff aware of the procedures?	Yes	
Are the DPO's details available on the website	Yes	
Data Security		
Is there a designated individual who is responsible for preventing and investigating security breaches?	Yes	Head Teacher
Is there a documented process for resolving security related complaints and issues?	Yes	
Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	Yes	Encryption, fire walls, egress etc are used



Is personal information (stored on cloud, computers etc) systematically destroyed, erased, or anonymised when it is no longer legally required to be retained.	Yes	Head checks with staff and systematically destroyed
Can access to personal data be restored in a timely manner in the event of a physical or technical incident?	Yes	All online/cloud based.

