Data Management

Brambleside Primary School

General Data Protection Regulations Audit

Ruth Hawker

Company Director

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

Becky Clark

Assistant Director

MAAT, Tech ISOH, MInstLM, AIIRSM

Contents

1.0 Overall Summary

1.1 Date of Audit and Key Information

Date	26th April 2023
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 organisation can show that it has taken appropriate practical steps outlined as necessary by the Information Commissioners Office.

2.0 School Details

School Name	Brambleside Primary School
School Address	Cleveland Avenue, Kettering, Northants, NN16 9NZ
Telephone Number	01536 310680
Head Teacher	Mr Drew Brown
Chair of Governors	Mr Bill Parker

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 approve.

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

4.1 School Audit Table

Compliance/Policies		
Do the Trust/School have:	**Answers:**	**Recommendations/ Comments:**
Data Protection Policy	The school have a Policy	Needs to be reviewed in April 23 and uploaded onto the website
IT and Acceptable Use Policy	No	
Data Breach Procedures	Breaches are included in the GDPR Policy	Produce a flowchart to show what to do in the event of a breach
Workforce, Pupil, CCTV, Governors/Trustees and LAC/CIN Privacy Notices	Privacy Notice for workforce, pupils and website are available on the school website. The schools do not have CCTV.	LAC/CIN and Governor Privacy notices are available from the Plumsun Portal.
Information Audit - reviewed regularly and up to date	The school have an information audit.	Need to review information audit to ensure it is up to date.
Retention Document - in line with the Information Audit	Retention of data document in school	Consider adopting the Plumsun retention document. Ensure this is in line with the information audit.
Record of Personal data that has been destroyed	No	Document any personal data destroyed going forward.
Consent Forms (In most cases not required)	Pupil permissions are requested for photographs.	Consider the use of a statement rather than asking for consent.
Record of Consent (If required)	Permissions are kept in an excel spreadsheet kept on a shared drive.	
Data Sharing Agreements with suppliers	No	Produce a list of contractors and ICO numbers
Record of Subject Access Requests	N/A	All SAR will be recorded going when required
Record of Data Breaches	N/A	Data Breaches will be recorded when required
Record of Data Protection Impact Assessments	No	Complete going forward

Record of Personal Data being removed from site	Not all documents are known	Trip documents to be considered, if hard copies removed from site, ensure they are signed out and in when the trip returns. Consider using computers or tablets.
Register of School IT Hardware (Laptops, Mobile Phones etc)	Yes, stored online	

Processing Data		
Do the Trust/School have:	Answers:	**Recommendations/ Comments:**
A Data Protection Lead who overseas data compliance and liaises with the external DPO	School Business Manager	
Where are Privacy Notices available, are they sent out with welcome packs	Pupil welcome packs	Staff privacy notices are not sent with application packs or inductions packs.
GDPR is a regular item on the Government Body agenda	Yes	
Personal data held on servers, computers etc is secure, firewalls are secure and hardware has encryption installed and doors are locked where necessary.	Yes - all secure, laptops are encrypted. Documents stored in locked cabinets	Ask IT to ensure laptops are encrypted
Only personnel who are required to access personal data are able, checks are made to ensure this	Yes - these are restricted by role.	
Subject Access Requests are processed in line with the GDPR Policy	None to date Plumsun support any SAR's	
Requests to exercise rights are processed efficiently and timely (Right to erase/correct)	Data collection sheets sent out annually. School have recently changed to Arbour….going forward parents will have access to change information with schools controls in place.	

Personal data has been erased in line with the retention document (Physical copies should be shredded, electronic data should be erased	Yes, completed annually	
Personal data is not held for 'just in case' purposes	No	
Annual checks are completed to ensure data is not being held unnecessarily	Yes	

Security of Documents (Physical and Electronic)		
Do the Trust/School have:	Answers:	Recommendations/ Comments:
Physical copies of personal data not left out when away from desk (Clear desk policy)	No – clear desk policy in place	
Personal data is stored securely when the building is closed and only personnel who require the data have a key	Yes – locked cabinets	
Only personnel who require access to personal data have a key/know where the key is stored	Yes	
ID is warn by members of staff at all time on site	Yes	
Visitors are signed in and out of the building	Yes	
All doors to offices are kept locked when not being used (where personal data is held)	Yes	
Windows are locked when the room is not in use	Yes	
Window restrictors are in place when open	Yes	
Displays around the school containing personal data only show essential information	Yes	
Sensitive data, required to be displayed, is kept away from the public	Yes	

Where sensitive data is displayed, is it covered or removed when/if the room is being used by others other than members of staff	Yes	
Screens cannot be seen by those other than staff	Yes	
Idle time is enabled	No	Staff lock their computers when away from their desk. Consider enabling idle time.
Access to electronic personal data is restricted by roles	Yes	
Passwords are in place for laptops, printers/photocopiers, access to software etc	Yes	
Sensitive documents are password protected	Yes	
Where sensitive documents are required to be sent, these are encrypted before sending and checks to the who the document is being sent to is checked	Egress is used and S2S is used.	
USB ports are locked down to prevent data being saved and being removed from site	No – required for Smartboards.	USB's are encrypted
Encryption is on all hardware (USB included)	Yes	
Personal emails are not used, Governors, Staff and Pupils have school email addresses	Yes, all staff, pupils and Governors have school email addresses	
Incoming emails are checked before opening to ensure the sender is known (avoids phishing and viruses)	Yes.	

Working Remotely		
Do the Trust/School have:	**Answers:**	**Recommendations/ Comments:**
Physical copies of personal data are stored securely and not in a vehicle when removed from site	N/A	
Electronic personal data is saved to the device and available via remote access	Yes	

Remote access devices are encrypted and any windows are closed when not in use	Cloud based applications which time out.	
Only personal data that is required to work remotely is removed from site	Yes	

Training		
Do the Trust/School have:	**Answers:**	**Recommendations/ Comments:**
All Staff, Governors and Volunteers receive annual GDPR training and evidenced recorded	No	
If a breach has occurred, additional training has been given and processes amended accordingly	N/A	
Staff have read and understood the GDPR policy and evidence recorded	No	
Additional training/exercises are completed throughout the year	No	

5.0 Appendix

5.1 Listings of documentary evidence

School Website reviewed
School admission form

5.2 Listings of observations

Limited data shown on displays

5.3 Listings of interviews

School Business Manager