

Name of Governor	Andrea Williamson
Date of Visit	17th March 2025
Agreed Focus for Visit (linked to SEF, SDP & Key priorities)	
Name of Staff	Jo Griffith
HUGG shared? (if subject area)	
Next Steps/follow up from previous monitoring Follow up to ensure the school are following GDPR policy and all data is stored with safety in mind. Review a recent SAR request. Ensure new systems are working and secure.	
SAR process for recent request - this is now completed This went via the RBWM allocated point of contact for this parent. Then sent to the Head and it was agreed that DPO at Borough that needed to decide the material and what to redact due to the Head's prior involvement. All information was sent to the DPO as per the points requested. The DPO then redacted as required to then send to the SAR applicant. It took the Head 2 weeks to access all the information. School had 20 calendar days including Half Term to respond. Any further communications will be between the parent and the DPO.	
Data security: Digital - Every staff member has their own One Drive which is backed up with user ID authentication. Office are on a separate server which staff cannot access. TSI are the internet provider. They maintain the servers. They do User ID Password re-authentication. Physical - pupil data is in the locked cupboard in the Heads' office. Folders in the Head's office and only the Head has access. The Head's team have a second key for required access in the event that the Head is not available. -Everything else is stored in One Drive on Staff Laptops. All pupil progress data etc. is all on cloud based information. -Transferring files - physical ones are taken to the school and signed for. CPOMS also offers the facility for safe electronic information. Any new pupil's information is shared. For a child on Child Protection as an example there might be paper. A note is made on CPOMS to refer to the information in paper. -Any internet searches done on our servers - list gets sent to the Headteacher daily. All data is stored with TSI. Link here -Arbor - Management System for registers, emails from the office, medical, SEN, parent account. Access is online with a secure log in. This is the system that most schools in the UK use. -CPOMS - this is the safeguarding tool. Every staff member has a log in. The 4 DSL's have a 2 factor authentication log-in. The Safeguarding Governors check this. SEND, Behaviour and Safeguarding are stored here. -Tapestry is used for Reception but this is self-consenting for the parents who determine what information. -Juniper Education run the website.	
Actions used to identify findings -Discussion with Head -Viewing Arbor in person -Seeing paperwork (did not access content due to Data Privacy) -Website. -I saw the SAR print out letter but did not read any of the other information as per Data guidelines. Anything physical data e.g. children's behaviour and attendance on paper is stored in the locked cupboard	
What outcomes have been identified as a result of my visit Data Retention Policy etc can be found on the school website with the DPO clearly named: Link here	

How I witnessed the vision in action during my visit (*'I know there is nothing better for people than to be happy and do good while they live.'* Ecclesiastes 3:12)

The school have a process in place and follow the Data Retention and associated policies. They are published on the website and I also saw evidence of a recently completed SAR.

Impact of this visit

The school have demonstrated adherence to the required policies. We went through different examples of where the policy has been followed following incidents/potential incidents.

Aspects I would like clarified/Questions I have

PTA Social Media Policy - this is governed by the Head but I did not see any of these. Perhaps a review for the next visit?

. There is no Social Media used in the school.

Classlist is used and follows the GDPR policies.

To be shared with the school staff and school Governing Board.

Signed:

(Governor)

Signed:

(Headteacher/Staff member)