Procedures for identifying and reporting of data breaches

All staff will be made aware of the GDPR Policy; Privacy notices will be distributed to all students/families & staff; and annual training regarding safety of data and data breaches will be part of the CPD process.

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Every half term, the SBM is to walk the site identifying any areas or practices of concern, in relation to data security. This could include, but is not restricted to, 'bin surfing' (paper waste check), computers locked, filing cabinets locked.

If a data breach has been identified, it should be reported immediately to the DPO (Cathy Bach), the Headteacher and the SBM. During holiday periods, if none of these post holders can be contacted, a member of SLT must be informed immediately.

The form (Appendix 2 of the GDPR Data Protection Policy) must be completed with full details of the actual/suspected breach.

WITHIN 72 HOURS following the reported incident, the school will collate the details, will investigate and after liaising with the Local Authority, decide if the incident is of sufficient severity to report to The Information Commissioners Office.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.