Terms of Reference for the GDPR Lead
West Hill Primary School

The GDPR lead governor is responsible for overseeing and scrutinising the school compliance with the data protection laws. To assist in this process, the governor should monitor and scrutinise the following:

1. The school is registered with the Information Commissioner's Office and pays the annual fee.

2. The school has appointed a knowledgeable and experienced Data Protection Officer, who is able to perform their duties independently and without a conflict of interest. The Data Protection Officer is provided with the necessary resources and support to fulfil their statutory duties under Article 39 of the GDPR and is able to report directly to senior management and the governing board when required.

3. Governors and senior management lead by example and actively promote a positive culture towards data protection compliance. This is demonstrated through regular meetings, discussions and communications sent to employees and governors, about the importance of handling personal data appropriately and securely.

4. The governing board monitors the school data protection compliance against a set of Key Performance Indicators. Key areas monitored may include requests, training and security incidents.

5. The governing board receives data protection compliance reports (at least annually), which highlight the school current compliance levels and any risks or areas of non-compliance.

6. A data protection compliance audit is carried out annually. The results from the audit are reported to the governing board and senior management team. The governing board monitors the school completion of actions arising from the audit, to ensure they are done so in a timely manner according to risk.

7. The governing board records and monitors the risks associated with data protection compliance and ensures appropriate mitigations are in place to reduce the likelihood of those risks materialising. Risks may include financial, reputational and damage to data subjects (material and non-material).

8. Data Protection Impact Assessments are carried out on high risk activities, particularly when using cloud technologies and due diligence checks are carried out on suppliers who receive personal data (data processors). Contracts are in place which contain appropriate data protection clauses.

9. The school has appropriate technical and organisational security measures in place to protect the school data. The confidentiality, integrity and availability of the school data is managed by knowledgeable and experienced IT professionals, who regularly report on threats, vulnerabilities and security improvements.

10. The school has a comprehensive Data Protection Policy, which sets out how the school manages personal data. This policy is published on the school website and reviewed on an annual basis. Employees and governors are required to read policy revisions and a record is maintained when they have done this.

11. New employees and governors complete mandatory data protection training when they join the school. Existing employees and governors complete refresher training on an annual basis. A record is maintained of when training has been completed on an individual basis.

12. The school provides data subjects with privacy notices when their personal data is collected. These notices are published on the website or provided directly to data subjects, including any revisions.

13. The school maintains an accurate record of its processing activities.

14. The school manages its records effectively through appropriate storage, filing/naming conventions, accessibility, data accuracy checks, security and disposes of records in line with a Record Retention Schedule.

15. Staff involved in the sharing of personal data with partner agencies, are given training and advice on when to share data, when consent is required and how to send the information securely.

16. The school has procedures in place to identify, manage, report and record personal data breaches.

This list is not exhaustive.