Report to:	**Schools Forum**
Date of Meeting(s):	**5 March 2020**
Subject:	**Internal Audit General Data Protection Regulation (GDPR) Thematic Review**
Report of:	**Mark Barrow – Audit Manager**
Contact Officer:	**Stuart Spore – Principal Auditor**

Summary:	To provide an overview of the Internal Audit GDPR Thematic review conducted against a sample of schools during 2019/20. Outcomes and recommendations for schools to consider as part of their Data Protection 2018 responsibilities.
Recommendation(s):	To recommend that schools perform a GDPR self-assessment, where not already undertaken.
Implications:	
*What are the **financial** implications?*	None
*What are the **staffing** implications?*	None
Risks:	Non-compliance with Data Protection Act 2018, which may result in poor data management controls resulting in: • Loss of data • Distress to data subjects • Reputation damage • ICO sanctions, i.e. financial and operational

Please list any appendices:-

Appendix 1 – GDPR Self-Assessment Framework

1. Introduction

1.1 Compliance with the Data Protection Act 2018 and General Data Protection Regulations 2018 (GDPR) is a statutory requirement and as such each school is a designated 'Data Controller' who must exercise overall control over the purpose for which, and the manner in which, personal data is processed.

1.2 As part of the Internal Audit service to schools a Thematic Review in respect of GDPR was undertaken during 2019/20, utilising the 2018/19 position.

1.3 On completion of the review the results have been distributed to all schools with a recommendation that they undertake a self-assessment to determine their level of compliance, where not already done so.

2. Audit Approach

2.1 A sample of 6 schools were requested to undertake a GDPR self-assessment as per the framework document supplied by Internal Audit (see Appendix 1). The sample selected included 4 Primary Schools, 1 High School and 1 Special School.

2.2 The self-assessment consisted of 26 questions covering 6 key areas, i.e.

1) Information You Hold
2) Lawful Basis for Processing Data
3) Rights for Individuals
4) Governance
5) Third Parties
6) Data Security and Data Breaches

2.3 The completed self-assessments were evaluated by Internal Audit to determine the level of compliance. Where documentation could be supplied to support the compliance stated this was also evaluated.

2.4 On completion of the evaluation a Thematic 'Dashboard' report was produced to highlight common areas of compliance and non-compliance, which aimed to assist schools in targeting key areas of risk.

3. Summary of Findings

3.1 Within each of the 6 key areas the evaluations showed that the following controls required attention:

1. Information you Hold:

Less than 50% of the schools had completed an information audit to document the personal data held and how this data flows into and out of the school.

2. Lawful Basis for Processing Data:

33% of the school's had not reviewed their process for asking for and recording 'consent' as a lawful basis for processing data.

3. Rights for Individuals:
Less than 50% of the school's had:
i) updated their Privacy Notices; and
ii) established a procedure for responding to individual's requests under GDPR.

4. Governance:
Less than 50% of the schools had:
i) shared an approved Data Protection Policy with staff.
ii) provided Data Protection training.
iii) established a Data Protection Impact Assessments process; and
iv) established a direct reporting line between the Data Protection Officer and the Governing Body.

5. Third Parties:
All six schools use a third party to process data, but only one had written contracts in place that specified the data processor's data security and audit arrangements.

6. Data Security & Data Breaches:
Less than 50% of the school's had:
i) approved an Information Security Policy and shared it with staff; and
ii) established a data breach procedure.

3.3 It should also be noted that at the time of the review a number of schools were in the process of outsourcing their data protection function and that additional controls may have been implemented as a result of this.

4. Key Recommendations

4.1 Schools should undertake a GDPR self-assessment to determine the level of compliance with the GDPR Regulation 2018 (Appendix 1).

4.2 The results of the self-assessment should be used by the school to implement processes and procedures needed to meet compliance.

The actions for implementation could be in the form of an Action Plan that should be regularly reported to and monitored by the Governing Board.

4.3 It should be recognised that the importance of maintaining effective data management controls is a continuous process, which should be supported by regular Governor and staff training and awareness.

APPENDIX 1

GDPR Self-Assessment Framework

Ref	Expected Control	In Place (Y/N/In Part)	Action Required	Responsibility and Target Date
1. Information you hold				
1.1	Has the school undertaken an 'information audit' to identify what data is processed and how this flows into, through and out of the organisation?			
1.2	Has the school documented the personal data that it holds, where this came from and how this data is used?			
2. Lawful basis for processing data				
2.1	Have the lawful bases for processing personal data been identified and has this been documented?			
2.2	a) Does the school use 'Consent' as the lawful basis for processing any personal data? If so: b) Has the school undertaken a review of its process for asking for and recording consent to ensure compliance with the GDPR?			
2.3	Has the school registered with the Information Commissioner's Office (ICO) and paid the appropriate fee?			
3. Rights for Individuals				
3.1	Has the school reviewed and updated its Privacy Notices to ensure compliance with the requirements of the GDPR?			
3.2	Where Privacy Notices are provided to Children, are these written in clear and plain language which is age-appropriate?			

Ref	Expected Control	In Place (Y/N/In Part)	Action Required	Responsibility and Target Date
3.3	Has the school established procedures for responding to requests from individuals relating to their rights under the GDPR? *(See Individuals Rights in Glossary at Appendix 1)*			
3.4	Does the school complete or intend to complete regular data quality reviews to ensure that the personal data held remains accurate and up to date?			
3.5	Has the school implemented a written retention policy or schedule outlining when data should be disposed and the method of destruction?			
4. Governance				
4.1	a) Has a Data Protection Policy been established by the school? b) Has the Policy been approved by the Governing Body?			
4.2	Has the Data Protection Policy been communicated to all staff?			
4.3	Has appropriate data protection awareness training been provided to all Governors and school staff?			
4.4	Has a process been established to identify and assess risks associated with personal data?			

Ref	Expected Control	In Place (Y/N/In Part)	Action Required	Responsibility and Target Date
4.5	a) Does the school understand when a Data Protection Impact Assessment (DPIA) should be conducted? b) Has a process been established for completing DPIA's together with the allocation of responsibilities?			
4.6	a) Has the school appointed a Data Protection Officer (DPO)? b) Did the Governing Body approve the appointment of the DPO?			
4.7	Has a process been established to monitor compliance with the Data Protection Policies?			
4.8	Does the DPO report directly to the Governing Body?			
5. Third Parties				
5.1	a) Does the school use any third parties to process personal data? If so: b) Is there a written contract in place with each data processor which includes specific terms ensuring that data processing meets the requirements of GDPR?			
5.2	Are the data security arrangements clearly documented in the contract and /or agreement with the data processor?			
5.3	Has the data processor been audited or provided evidence to the school to demonstrate that the security controls are operational?			

Ref	Expected Control	In Place (Y/N/In Part)	Action Required	Responsibility and Target Date
6. Data Security and Data Breaches				
6.1	a) Has the school developed and implemented an Information Security policy? b) Has the Governing Body approved the Information Security policy?			
6.2	Has the Information Security Policy been communicated to all staff members?			
6.3	Are checks undertaken to confirm that data security controls are operating effectively?			
6.4	a) Has training been provided to staff members on how to recognise and report data breaches? b) Is training to be provided on a regular basis?			
6.5	Has the school established a documented process for investigating data breaches?			