Shared Internal Audit Service
Hertfordshire in Partnership

Draft Internal Audit Report

Themed Audits – GDPR in Schools

2018/19

Audience:	**All Maintained Schools**
Date of Publication:	November 2019
Reference:	SCH92/18/001

INDEX

1. EXECUTIVE SUMMARY

Introduction

1.1 The Shared Internal Audit Service (SIAS) provides internal audit services to Hertfordshire's maintained schools. Hertfordshire County Council's Schools Audit Strategy includes a requirement to annually establish the effectiveness of financial control, risk management and governance arrangements in a sample of schools. A review of School compliance with the General Data Protection Regulations (GDPR) has been included as one of the approved audit themes in 2018/19.

1.2 GDPR is new legislation governing data protection. It incorporates the principles of lawful processing from the Data Protection Act 1998, but also includes changes to what is classed as personal data and regulates the use of personal data. Schools were required to comply with this legislation from 25 May 2018.

1.3 Within this audit SIAS visited 14 schools to evaluate the systems in place to manage the compliance to the GDPR legislation, with compliance testing undertaken to validate responses provided by school staff. Each school visited was issued with an individualised report which provided detailed outcomes from the audit visit, and assurance regarding the effectiveness of its internal controls in the audited areas. Recommendations were given where required, to improve the internal control arrangements.

1.4 Our specific objective in undertaking the GDPR in schools audit was to provide the Council and the sample of schools visited with assurance on the effectiveness of internal controls, processes and records in place to mitigate risks in the following assurance areas:

- Policies, Procedures and Training
- Governance
- Subject Access Requests (SAR's)
- Third Parties
- Data Audit
- Data Retention and Privacy Notices

1.5 For the benefit of all maintained schools, we have provided in Appendix A, a summary of findings and reminders of good practice that were identified during school visits. It is recommended that all schools use the appendix to self-assess the robustness of their existing systems for complying with the GDPR legislation.

1.6 Appendix D gives a breakdown of the assurance levels awarded for the individual assurance areas at each school. This highlights the areas that schools may wish to focus on when reviewing their compliance.

This section summarises the findings from the 14 schools audited, which individual schools may wish to use to self-assess the robustness of their own internal control framework for GDPR.

Ref	Finding	Recommendation
1.	**Internal GDPR Policy** During our visits to the sampled schools we identified one instance where a school did not have a specific internal GDPR policy document. In the absence of such a policy we also noted that GDPR was also not covered in any other relevant policy, such as the data protection policy. <u>Associated Risk</u> Without a GDPR policy being in place there is an increased risk that staff would either not be aware of their obligations, or would not have a reference point to identify key requirements.	Schools are reminded of the importance of having a specific internal GDPR and related policies (such as data protection), and ensuring that these have been circulated to and read by all staff. We highlight that as a minimum the GDPR policy should contain the following elements: • Policy statement and objectives • The status of the policy • The role of the DPO • Definitions of terms • Data protection principles • Lawful basis of consent • Purpose of holding data • Security • Data Subjects' rights • Issuing information / Disclosures • Accountability • Document Control Section

Ref	Finding	Recommendation
2.	**Physical Data Security** During one of our audit visits, SIAS identified that some personal data was kept in unlocked cupboards, within a room that is not secured. <u>Associated Potential Risk</u> Where physical data, such as forms and records, are not properly secured there is a risk that staff or visitors not entitled to see such information may access it. In extreme circumstances, where information is of a sensitive or confidential nature this could constitute a data breach.	Schools are reminded of the importance of having robust arrangements in place to safeguard the security of physical data, ensuring that any areas where personal data can be held (either physically or online) are properly secured and access only given to relevant members of staff. We also highlight that it would be best practice to periodically test the robustness of such arrangements (such as clean desk policies), to ensure that staff are complying with the arrangements put in place.

Ref	Finding	Recommendation
3.	**Review Dates on Policy** Whilst the large majority of schools visited had appropriate policies, guidance and key forms in place, none of those visited had either included review dates on the document, or incorporated a periodic review into document review schedules. In making the above observation, we highlight that as the GDPR legislation only came into force in 2018 this was not considered an issue at this point in time, but would be if policies were not routinely reviewed in the longer term. <u>Associated Risk</u> If systems are not in place to prompt policy or key document reviews these are likely to become quickly out of date and potentially no longer align to relevant legislation. In extreme circumstances this may increase the risk on non-compliance through unawareness of changes to key requirements.	Schools are reminded of the importance of undertaking regular reviews of their GDPR Policy, Data Audits and other key documents or templates associated with systems to comply with the regulations. In order to avoid the risk of this being overlooked we advise schools to include review dates on key policies, records, audits and forms to ensure that prompts are in place to review them. In addition, schools may wish to add the review GDPR records, policies and forms to the annual policy review calendar / programme of business.

Ref	Finding	Recommendation
4.	**Staff Inductions** During our audit we reviewed the area of staff induction, this being key to ensure that staff are aware of their responsibilities at the outset of employment. Whilst all schools visited were found to have an induction process in place, there were some instances where these did not include a section on GDPR. <u>Associated Risk</u> If new members of staff are not aware of their responsibilities in relation to complying with the GDPR, there is an increased risk that the school may be subject to a data breach which could carry financial or reputational damage.	Schools are reminded of the importance of including the GDPR within induction programmes for new staff. This should include the requirement for new staff members to read the GDPR policy and any associated policies such as data protection. The staff induction pack should include a checklist of information to be covered, with completion being checked before this is signed off. To ensure that the school can evidence that they have provided new staff with the appropriate induction and training in the GDPR, a copy of the completed induction checklist should be retained in their personnel file. Schools should also consider adding a section that references the GDPR within any staff handbooks that may be in place.

Ref	Finding	Recommendation
5.	**Consent** Whilst only identified within one of the schools visited, we identified an instance where a school had created a “Take-Home Teddy Bear” activity, this involving the completion of a page of a journal, with photographs, to record activities undertaken whilst at home. However the journal, by concept, is passed (upon completion) to a different child and parent to add their entries. The school raised concerns as to whether the introduction of the GDPR may create issues with the above activity. In response to this query we have advised the school that it may be more appropriate to simply ask children / parents to complete individual sheets for the activity, with these being collated and retained in school for classroom use only. Should the school decide to continue with the current approach we recommended that further advice is sought from their DPO, as the school may be required to obtain consent forms from parents and others on any photographs to confirm that they agree to the sharing of photographs or individual entries. We also identified further instances where consent was not obtained in the expected manner. We were informed that for a school journey, where the sharing of personal data was required, consent was obtained during a meeting, rather than through written consent. A parent could claim for data breach and in the absence of proof of consent this could negatively impact on the reputation of the school.	Schools are reminded of the importance of ensuring that the extent of sharing data, photographs, or information personal to an individual is carefully considered within the planning of school activities. Where the school are unsure whether the activity would require consent from those involved, they should seek advice from their DPO. Schools are also advised to seek advice from their DPO where they plan to use more “informal” methods for obtaining consent, thereby ensuring that this will be compliant with the GDPR. Finally, where a school intends to use consent for a specific purpose that will remain in force during a child’s duration with the school, this must be made clear to the person providing consent on the form they are being asked to sign.

Ref	Finding	Recommendation
	Finally, we identified an instance where consent had been obtained and the school had considered that these would remain in force throughout the child's duration at the school, but this had not been made clear on the form. <u>Associated Risk</u> Schools may inadvertently breach the GDPR by sharing photos or information without an individual's consent. In extreme circumstances this could lead to claims of a failure to comply with GDPR.	

Ref	Finding	Recommendation
6.	**GDPR Training Record** Whilst the majority of schools visited were able to provide evidence that all relevant staff had received appropriate training in relation to the requirements of the GDPR, we identified in one school a formal record of who had attended the training delivered had not been maintained. In addition, we also noted for a further school that it had not been possible to deliver the initial GDPR training to some staff members as they had not been at work on the day it had been delivered. <u>Associated Risk</u> If a significant data breach occurred the school would need to demonstrate that they had satisfactorily trained all staff in the requirements of the GDPR, which may not be possible if appropriate records are not maintained.	Schools are reminded of the importance of ensuring that all staff have received appropriate training on the GDPR, as well as any associated training for various more specific elements of the legislation (such as data protection). In the event of a data breach it would be important that the school would be able to evidence that all staff have received the training, therefore ideally a training record should be maintained that records the date of attendance, or as a minimum attendance sheets should be retained to support the training session records. Schools should also ensure that appropriate arrangements are put in place to provide training to staff who may not have been present when the original training was delivered. Finally, schools should ensure that periodic refresher training is delivered to both update staff on any changes to requirements in future years, or purely to refresh their knowledge.

Ref	Finding	Recommendation
7.	**Up to date information** Within one of the schools visited during the audit we were informed during the review that a specific DPO email address has recently been set up for GDPR, however existing documents still currently include the previous admin e-mail contact address. Whilst the above is a minor example of key documents not being updated, other audits performed by SIAS, such as SFVS have highlighted several occasions where schools have failed to personalise policies to school when downloading from the Grid. <u>Associated Risk</u> Where generic policies are not reviewed prior to being adopted there is a risk that elements may either not be relevant or may be mis-interpreted by those required to abide by the policy.	Schools are reminded of the importance of ensuring that any template policies or documents are sufficiently reviewed and personalised to their school, prior to adoption. Governors should also be reminded to ensure that this is the case, prior to approving any policies that are presented.

Ref	Finding	Recommendation
8.	**Compliance of Third Parties** One of the areas covered during our audit visits was to assess the actions schools had taken to make third parties aware of any revised expectations following the introduction of the GDPR. We identified that whilst the large majority of schools were aware of the contract variation template that is held on the Grid, schools were at various stages in relation to issuing these to the third parties, with some having fully completed this task, some in progress and also a small number of schools who had not commenced this process. We also noted that whilst some schools had also looked to review the GDPR policies of those third parties that used school data to perform their services, this was the not case for all schools. Finally, we identified a small number of schools that did not have an up-to-date contract register, therefore making it more difficult to obtain assurance that contract variations had been sent to all relevant third parties. <u>Associated Risk</u> If third parties are not made aware of their revised obligations as a result of the introduction of the GDPR, there is an increased risk that they may not comply with them. This could equally enhance the risk of a data breach or non-compliance with the regulations occurring.	Schools are reminded of the high importance of ensuring that all third parties that may have access to, or need to process school data as part of delivering their services have been issued with a contract variation letter which makes them aware of any revised obligations. These contract variations should be signed by Third Parties and held on record by the school. In addition, schools are reminded that it is good practice to obtain assurance that third parties used have appropriate policies and procedures in place that promote compliance of the GDPR by their staff. Finally, schools are reminded that contract registers should be kept up to date and be periodically checked for completeness. This will ensure that they are sufficiently accurate for both financial and contract monitoring purposes, as well as being a record that can be used to identify those third parties where contract variations may need to be issued.

Ref	Finding	Recommendation
	Without contract amendment clauses being issued to, and signed by third parties, the school will remain entirely responsible for any error which the data processor makes. This could result in enforcement action by the ICO.	

Ref	Finding	Recommendation
9.	**Data Protection Impact Assessment** The completion of data protection impact assessments was found to be variable amongst the schools sampled, with some having a fully completed assessment, whilst a small number of schools were yet to complete this task. <u>Associated Risk</u> In the absence of a fully completed DPIA, schools may not have robustly assessed the data protection risks they face and how these can be mitigated.	Schools are reminded of the importance of completing Data Protection Impact Assessments (DPIA) to assist in the identification and minimisation of data protection risks. Schools should be aware that DPIAs are a legal requirement for processing activities that are likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping demonstrate accountability and building trust and engagement with individuals. The DPIA should: • Describe the nature, scope, context and purposes of the processing; • Assess necessity, proportionality and compliance measures; • Identify and assess risks to individuals; • Identify any additional measures to mitigate those risks.

Ref	Finding	Recommendation
10	**Completion of a Data Audit** For a small number of schools visited during the audit review we identified that they were yet to complete a data audit, or that such an exercise was currently in progress (in varying stages of completion). <u>Associated Risk</u> In the absence of the completion of a data audit the school will not have a full awareness of the data that it handles and the legal basis for doing so. This increases the risk that the school will be unable to fully comply with the GDPR.	Schools are reminded that the completion of a data audit should be the initial task for preparing for compliance with the GRPR. For any schools that have not completed a data audit this should be seen as an immediate priority. We also highlight that as good practice for governors, confirmation should be sought that a data audit has been completed, or where this is currently in progress appropriate oversight should be maintained to ensure that this exercise is completed at the earliest opportunity. Finally, schools are reminded that the data audit should be periodically refreshed to ensure that it continues to reflect the data handled by the school.

Ref	Finding	Recommendation
11.	**Data Retention** As part of assessing how schools manage data held, we sought to obtain assurance that data retention schedules were in place. For one of the schools visited we identified that whilst they had a data retention policy, this was not specific to the school and the data they held and had not been subject to recent review. We were also informed by one school that whilst they had a clear data retention policy and complied with this, further work was required to rationalise historic data on pupils and staff currently retained on both SIMS and individual teachers drives. <u>Associated Risk</u> In the absence of an up to date data retention schedule, staff will be unable to ensure that data is managed effectively. This may result in schools retaining information for longer than is necessary, which will result in non-compliance with the GDPR.	Schools are reminded of the importance of having an up to date data retention schedule, tailored to the specific needs of the school. This should outline the data retention period for certain documents expires (based on the 'reasonable length of time' guidelines) and legal requirements. When the data retention threshold is reached, the data should be securely disposed of. Schools are also reminded that the process of disposing of data in line with their data retention policies also applies to data held on electronic systems, including the computers held by individual staff. It would be considered best practice for an annual process to be in place for disposing of data from both the central records and the individual drives of the staff.

School	a) Policies and Procedures	b) Governance	c) Subject Access Requests	d) Third Parties	e) Data Audit	f) Data Retention and Privacy Notices
A						
B						
C						
D						
E						
F						
G						
H						
I						
J						
K						
L						
M						
N						

Key: Overall Assurance Level issued to the individual schools in their reports

Good Satisfactory Limited No