Schools Themed Audit - GDPR

City of York Council

Internal Audit Report 2018/19

Business Unit: Children, Education and Communities Directorate,
Responsible Officer: Assistant Director Education & Skills
Service Manager: Head Teachers
Date Issued: 28/05/19
Status: Final
Reference: 15699/024

	P1	P2	P3
Actions	**0**	**1**	**2**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

The General Data Protection Regulation (GDPR) came into force on 25th May 2018.
Previous Data Protection Act (DPA) regulations ensured personal data was handled lawfully but GDPR requires the documentation of how and why all personal data is processed, and gives enhanced rights to the individual. All organisations including schools must have policies and data management procedures in place to ensure compliance with GDPR.

Objective and Scope of the Audit

The purpose of this audit is to provide assurance to management that the maintained schools have systems and controls in place to ensure compliance with GDPR and have:

- appointed a suitably qualified Data Protection Officer (DPO)
- provided adequate staff training on GDPR awareness
- produced an information asset register and have documented systems used to process personal data and mapped how this data is transferred to other systems or any third parties
- agreements in place for third party processors to ensure GDPR compliance
- issued privacy notices and updated consent forms to meet GDPR requirements
- compliant policies covering Information Management and Security, Data Breach Management, Acceptable Use and CCTV (if applicable)
- documented systems for dealing with data subject rights
- an up to date retention schedule and records of deletion

There are a number of external providers of Data Protection Officer services available to schools. However, most council maintained schools have chosen to appoint the Veritau Information Governance service to provide support and to act as DPO. The audit reviewed the controls in place in those schools that haven't elected to use this service, to ensure they have equivalent processes in place. This was, initially via questionnaire, followed by a review of evidence to support the responses received

Key Findings

Of the four maintained schools not appointing Veritau Information Governance Service to act as their DPO, three had appointed their School Business Manager as their DPO and one was using the DPO arrangements for the MAT they were due to join.

Schools indicated from their response to the GDPR questionnaire that they had made good progress in introducing procedures and controls to ensure compliance with GDPR and were able to evidence this through the documents requested to support their responses.

All had provided GDPR training for their staff, had reviewed their agreements with third party processors, updated consent forms and issued revised privacy notices to their pupils and their employees. With the exception of one school, all schools had replaced their data protection policies with a GDPR compliant policy. In addition all schools had an acceptable use policy which was acknowledged by staff and had adopted a retention schedule.

However, it was found that:

- for all schools with an internally appointed DPO, the training for the role was limited did not appear to be detailed enough to meet advised standards.
- for one school GDPR compliant information and data security policies had not been adopted.
- in the absence of their DPO one school could not provide evidence of a completed information asset register.
- two schools did not retain evidence of the destruction or archiving of records at the time of audit.

Advice was provided to individual schools as part of this audit

Overall Conclusions

It was found that the arrangements for managing risk were satisfactory with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1 Data Protection Officer (DPO)

Issue/Control Weakness	Risk
Training for the DPO was found to be limited and may be insufficient for the role. Additionally, in the absence of the DPO data protection issues may not be correctly dealt with or the required registers maintained.	The DPO may have insufficient knowledge to promote an effective data protection culture within the school and enable compliance with GDPR.

Findings

In three of the schools reviewed the DPO was the School Business Manager. In the fourth school DPO services were being provided by the Trust the school was due to join.

As highlighted in the DfE toolkit for schools, although ICO does not require a qualification necessary for the DPO, there is published guidance on the level of expertise required, the expected position of the DPO within the organisation and the level of independence required. The level of expertise is not strictly defined but the DPO should have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the school and should have expert knowledge of data protection law and practice. The role should be independent (reporting to the highest level), and adequately resourced.

The level of training for the DPO's at schools varied but in all cases was no longer than a day (in addition to the general school training completed by all staff) and all courses were uncertified. This would appear to be insufficient for the role of DPO.

In one school the DPO was absent and a number of documents and registers required by the audit to assess compliance could not be located (including the information asset register). As a number of processes governed by the legislation are time sensitive schools should ensure date protection issues can be dealt with and relevant documents and registers accessed in the absence of the DPO.

Agreed Action

One of the three schools with their School Business Manager as DPO has now appointed Veritau to provide their DPO services. We will share the audit report with the Chair of Governors of the other relevant schools and remind them of the importance of assessing the risks associated with the School Business Manager covering the role of the DPO. We will provide details of where they can procure appropriate training for anyone providing the DPO role.

Priority	2
Responsible Officer	School Business Support Manager and schools Chair of Governors
Timescale	31`July 2019

2 Policy

Issue/Control Weakness	Risk
For one school the information and data security policies did not appear to have been updated to ensure compliance with GDPR. None of the schools reviewed had a specific data breach management policy in place but all had written guidance.	Policy and procedure at the school may be unclear or fail to comply with GDPR requirements.

Findings

A GDPR compliant data protection or information security policy did not appear to be in place for one school. The schools website indicated that policy was currently under review. The review had not been re-scheduled to take account of the introduction of GDPR.

None of the schools reviewed had adopted a specific data breach management policy, however all had written internal data breach reporting guidelines. These covered the detection of data breaches, investigation and internal reporting, as well as setting out the process for deciding whether reporting to the ICO is necessary (which must be done within 72 hours of detection of the breach).

Agreed Action 2.1

We will share the audit report with the Chair of Governors of the relevant schools bringing to their attention the risks associated with this control weakness and provide useful links for them to refer to. We do not propose to share this report with one school that has since converted to an academy which has its own GDPR arrangements in place.

Priority	3
Responsible Officer	School Business Support Manager and schools Chair of Governors
Timescale	31 July 2019

3 Destruction and Archiving of Records

Issue/Control Weakness	Risk
Two schools did not evidence that their records had been destroyed or archived in compliance with their retention/destruction schedule.	Failure to comply with GDPR in relation to the retention of records.

Findings

All the schools reviewed had a retention schedule in place. However at two schools there was no evidence to confirm the destruction or archiving of records and documents in accordance with the schedule.

All schools should have a process in place for highlighting documents due for destruction or archiving (both paper and electronic) and for recording documents destroyed. This should include a system that allows files to be monitored to ensure that documentation is not being incorrectly retained.

Agreed Action 3.1

We will share the audit report with the Chair of Governors for the relevant schools bringing to their attention the risks associated with this control weakness and provide useful links for them to refer to in respect of records management in schools.

Priority	3
Responsible Officer	School Business Support Manager and schools Chair of Governors
Timescale	31 July 2019

Annex 1

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.