Information Governance in Maintained Schools (follow-up)

City of York Council

Internal Audit Report 2017/18

Business Unit: Children, Education and Communities Directorate,
Responsible Officer: Assistant Director Education & Skills
Service Manager: Headteachers
Date Issued: 08/06/18
Status: Final
Reference: 15699/021

	P1	P2	P3
Actions	**0**	**3**	**1**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

The Information Governance themed audit follow up was agreed as part of the 2017/18 audit plan for Children's Services, Education & Skill. A previous audit was carried out in 2015/16 where limited assurance was provided.

Objectives and Scope of the Audit

The purpose of the audit is to provide assurance to management that the weaknesses identified in the 2015/16 audit have been addressed. We then conducted a review of the steps taken to ensure compliance with the key requirements of the General Data Protection Regulations (GDPR) to be introduced May 2018

Visits were completed to a sample of 10 maintained schools to ensure they;

- were aware of the weaknesses identified in the 2015/16 review
- have completed an ICO data protection self assessment or otherwise reviewed their current processes
- have an action plan to address any outstanding issues
- have the following key controls in place:
    - Schools are registered with the Information Commissioner as data holders.
    - A Senior Information Risk Owner (SIRO) has been appointed and they have received appropriate training.
    - Staff are aware of their Data Protection and Security procedures and requirements.
    - Policies are in place to comply with the various requirements.
    - Personal data is stored securely and retained only in line with guidance.
    - Back-up of electronic data procedures are in place
    - A Publication Scheme has been adopted and published
    - Privacy Notices (for both staff and pupils etc) have been made available, using the DfE model/standard document.

An Information Governance Audit Questionnaire was issued to all maintained schools.

The questionnaire established whether schools;

- are aware of the GDPR regulations including the need to appoint a Data Protection Officer (DPO)
- have communicated this with Governors

- have followed the ICO's preparing for GDPR 12 point plan
- have completed the ICO's GDPR readiness assessment
- have in place a programme/schedule of appropriate training for staff

Key Findings

Maintained schools received a copy of the report on Information Governance in Schools 2015/16 in November 2016 with advised actions to address the reported weaknesses. In November 2017 the report and advised actions was re- issued to schools in the York Education Newsletter as part of an information governance resource pack.

Our visits to ten maintained schools found that procedures appeared to have improved since the 2015/16 review although not all issues had been addressed. Only one school confirmed they had completed an independent self assessment of their Information Governance procedures. Others had viewed the report and assessed if any action was necessary.

All schools visited had reviewed their information security policies since the 2015/16 audit and were in the process of reviewing their policies again for compliance with GDPR. All were aware of the GDPR 12 point action plan and were progressing against this. Procedures were in place to ensure staff had read relevant policies and acceptable use agreements were in place for staff and pupils (apart from three schools where advice was given).

All schools had a named SIRO. The SIRO had received specific training for the role in only two schools but all were aware of the duties. Staff with responsibility for dealing with SARS and FOI requests were aware of the procedures to be applied. Data Protection Certificates were up to date and Privacy Notices in place for pupils though not always issued to staff (it is recommended they are published on the schools website). Schools were confident in their data back up procedures and the personal records tested were found to be stored securely.

Some schools had not published a model publication scheme and/or the accompanying schedule of information or adopted a data breach management policy. At two schools personal data was not held on encrypted portable devices. At all schools there was no evidence held to confirm the operation of an effective records management system. Schools generally had not completed a review of what data they shared to ensure all relevant contracts include assurance of DPA compliance and that data sharing agreements were in place for third party processors. These issues are detailed in the main body of the report.

A summary of the results of the questionnaire issued to all maintained schools is included as Appendix 1.

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 Freedom of Information Policies and Data Breach Management

Issue/Control Weakness	Risk
Some schools did not have policies and procedures in place that adequately covered data protection and Freedom of Information requirements.	The school may not be complying fully with the requirements under the Data Protection Act (DPA), Environmental Regulations (EIR) and Freedom of Information Act (FOIA). Failure to address Information Security Risks could result in breaches and financial penalties from the Information Commissioner.

Findings

Of the ten schools visited, all had reviewed their information governance and security policies since the previous audit. All schools had a procedure (within the school's Data Protection Policy) for responding to SARS and FOI requests and a named officer to whom all FOI and SARS requests were referred However it was found that :

- Two schools had not published the Information Commissioners Model Publication Scheme on their website but had published the Schedule of Information, one school had not adopted the Schedule of Information and one school had neither of these documents.

- Seven schools did not have a separate Data Breach Management Policy. The other three schools had included this within their revised Data Protection Policy.

Agreed Action 1.1

Each school is its own data controller and is legally responsible for complying with data protection legislation.
Since this audit was conducted we have provided guidance for head teachers at a briefing which took place on 8th May 2018. The slides have been shared with all schools. We will share the results of the audit with head teachers and chairs of governing body's and include a details of where schools may seek support for setting in place a data breach management policy. All schools already have access to resources through the York Education website which includes templates to adopt and support which they may choose to purchase.

Priority	2
Responsible Officer	School Head Teachers / School Business Support Manager
Timescale	May / June 2018

2 Records Management

Issue/Control Weakness	Risk
Schools were unable to evidence destruction or archiving of records in accordance with document retention schedules.	Current records management procedures may not comply with information security/Data Protection Act (DPA) requirements.

Findings

Record management procedures at all schools did not evidence that both physical and electronic records, are destroyed or archived in accordance with the schools document retention schedule.
Additionally, one school did not have a document retention schedule in place.

Agreed Action 2.1

We will remind schools of the importance of having document retention schedules in place and keeping evidence that both physical and electronic records are destroyed or archived. This will including sharing with them the records management tool kit for schools published by the Information and Records Management Society.

Priority	3
Responsible Officer	School Business Support Manager
Timescale	June 18

3 Encryption of Portable Devices

Issue/Control Weakness	Risk
Data held on portable storage devices such as laptops and memory sticks was not adequately protected at all schools.	If the unencrypted laptop or other assets holding confidential or sensitive information is lost or stolen this would be a data protection breach notifiable to the Information Commissioner and sanctions may be incurred.

Findings

Whilst the majority of schools ensured that any IT equipment staff use for work purposes such as laptops or memory sticks were encrypted, two schools had laptops that could be used to hold personal data that were password controlled only. These laptops were not taken off site, however, they were still vulnerable to being lost or stolen.

Agreed Action 3.1

We will remind schools of the importance of having all portable devices encrypted, even if they do not hold personal information.

Priority	2
Responsible Officer	School Business Support Manager
Timescale	June 18

4 Data Sharing Protocol

Issue/Control Weakness	Risk
Information shared with other data controllers may not be adequately protected and may be used for unauthorised purposes.	Failure to comply with the legal duty to protect data.

Findings

It was found that most of the schools visited had not completed a review of what data is shared, with whom and for what purpose, although assurances were given that that this review was in progress.

The schools could not therefore be sure that all the required information sharing agreements with third party data processors were in place or that contracts included adequate assurance of DPA compliance. Schools were unclear about which contracts this may apply to and were in need of additional support and guidance in this area.

Agreed Action 4.1

Since this audit was conducted we have provided guidance for head teachers at a briefing which took place on 8th May 2018. The slides have been shared with all schools. At the briefing schools were reminded to complete a data map and use this to prepare an information asset register. We will also share the results of the audit with head teachers and chairs of governing body's and include guidance on information sharing agreements. All schools already have access to resources through the York Education website which include templates to adopt and use.

Priority	2
Responsible Officer	School Business Support Manager
Timescale	June 18

Appendix 1

Questionnaire Results – Preparing for GDPR

The questionnaire was sent to 38 maintained schools. 23 responses were received during April 2018.
Of the completed responses:

- All schools were aware of GDPR
- All schools were aware of the requirement to appoint a DPO
- Two schools had not communicated this to Governors
- 8 had not appointed a DPO at the time of completing the questionnaire (3 of these schools did not answer further questions)
- 18 schools confirmed they were using GDPR preparation check lists
- 14 schools stated that staff had or were due to have GDPR compliance training (The rest either were waiting for advice/training from their appointed DPO service provider or had not responded to the question)
- Two schools felt there was a general lack of guidance and support on GDPR from the LA

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.