Annex 5

Themed Audit Information Governance

City of York Council

Internal Audit Report 2015/16

Business Unit: Children's Services, Education & Skills,
Responsible Officer: Assistant Director Education & Skills
Service Manager: Headteachers
Date Issued: 13/10/2016
Status: Final
Reference: 15699/009

	P1	P2	P3
Actions	**0**	**4**	**4**
Overall Audit Opinion	Limited Assurance		

Annex 5

Summary and Overall Conclusions

Introduction

The Information Governance themed audit was agreed as part of the 2015/16 audit plan for Children’s Services, Education & Skills to try and gauge the level of understanding of Data Protection and Freedom of Information requirements within City of York Council schools.

Objectives and Scope of the Audit

The purpose of the audit was to provide assurances to management that the processes that schools have implemented to manage key requirements in compliance with Data Protection and Freedom of Information Acts are effective.

An initial Information Governance Audit Questionnaire was issued to 20 randomly selected schools.

The questionnaire covered the following key controls:

- Schools are registered with the Information Commissioner as data holders.
- Schools have appointed a Senior Information Risk Owner (SIRO) and they have received appropriate training.
- Staff are aware of their Data Security procedures and requirements.
- Policies are in place to comply with the various requirements.
- Data is stored securely and retained only in line with guidance.
- Back-up of electronic data procedures are in place

Key Findings

20 schools were issued with a questionnaire. 5 schools failed to return these questionnaires despite subsequent reminders
The key findings taken from the 15 returned questionnaires and some limited additional testing included:

All schools who responded had procedures in place to ensure that staff were aware of their responsibilities regarding data security and e-mail and internet acceptable use.

All schools ensured that personal data relating to children and staff was kept up to date.

All schools had anti-virus software firewalls and filters on their ICT network.

All schools ensured they had permission from parents before allowing children to be photographed.

However several schools did not have appropriate policies in place to comply with legislation.

Schools were not generally aware of the term SIRO and their role and responsibilities prior to the audit.

Schools did not evidence that they had disposed of records in accordance with document retention schedules and a small number of schools were not clear on how long to retain personal files of staff and children.

At least a third of schools could not confirm that back-up data was tested to ensure its functionality.

Around a third of schools did not have encrypted memory sticks or laptops.

Data sharing protocol agreements were not in place to govern the work of any third party data processors.

Overall Conclusions

It was found that the arrangements for managing risk were poor with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided Limited Assurance.

1 Data Protection Roles and Responsibilities

Issue/Control Weakness	Risk
Although the majority of schools identified their Headteacher as their SIRO they were not generally aware of the term Senior Information Risk Owner (SIRO) and their role and responsibilities.	Data Protection and information governance may not be effectively managed.

Findings

Every school should have a member of staff, who has overall responsibility for information risk to ensure information relating to both teaching staff and pupils is managed securely. This person is the designated Senior Information Risk Owner (SIRO). It was found that of the 15 schools returning their questionnaire:

- Nine schools were not aware of the term SIRO prior to receiving the questionnaire, however fourteen schools named the Headteacher or School Business Manager as their SIRO. Guidance states that the SIRO must be an executive operating at Board level. In a school environment it is unclear if anyone other than the Headteacher has sufficient seniority to fulfil this role.

- No training for this role was identified as having been completed by these officers.

Agreed Action 1.1

Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.

Priority	2
Responsible Officer	Children's Services /School(s) / Head teacher(s)
Timescale	31st July 2017

<u>Actions for Schools</u>

1. To understand role of SIRO and provide at each school.
2. Training needs to be identified at school(s) and then a programme of training to be provided which must be recorded / evidenced.

2 Data Protection and Freedom of Information Policies and Procedures

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

Part of a schools compliance with the Data Protection and Freedom of Information legislation is to implement an Information Policy, adopt a Publication Scheme and to issue Privacy Notices parents and staff. A number of schools were not clear whether they had policies in place that adequately covered the security and management of records. A review of policies at several schools identified that most policies did not adequately cover the security of physical records, the removal of images from peripheral devices and guidance to staff on changing passwords. Of the fifteen schools returning questionnaires:

- Four schools had not adopted their own information management/data protection policy. It was noted that the model policy for schools is a number of years old and makes no reference to the role of SIRO.
- One school had not required staff to acknowledge the e-mail and internet acceptable use policy and seven schools had not periodically renewed this acknowledgement.
- Nine schools had no procedure in place for investigating and responding to security incidents.
- Three schools stated they had no monitoring procedure to ensure compliance with school policies.
- Five schools had not adopted the Information Commissioners Model Publication Scheme. Of those who had, four had not published the scheme and guide to information on their website.

Agreed Action 2.1

Agreed Action 2.1		
Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the	**Priority**	2
	Responsible Officer	Children's Services /School(s) / Head teacher(s))

first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.	**Timescale**	31st July 2017

Actions for Schools

1. Adopt and publish their Publication Scheme based on (as a minimum) the Information Commissioners Office (ICO) model publication scheme for schools
2. Undertake a review of required information governance and security policies and procedures and implement either new or up to date ones
3. Implement a method of monitoring and recording that their information governance and security policies and procedures have been read and understood by all staff & governors.
4. To introduce (or review their existing one) a data breach management policy/procedure in their school
5. Introduce (or review existing) retention policy/procedures and retention schedules for their records
6. Introduce or review the policies/procedures for responding to both FOI and Subject Access to Records (SARs) requests

3 Freedom of Information and Subject Access Requests

Issue/Control Weakness	Risk
A designated person and a deputy had not been appointed in all schools to champion and coordinate information management and process information requests.	Information requests may not be passed to the appropriate officer to ensure they are properly addressed within given timescales.

Findings

All schools confirmed that they had a system in place to ensure requests for information received (including subject access requests and freedom of information requests) were logged and responded to within the appropriate deadlines. However, five schools did not name a designated officer who would take responsibility for dealing with these requests.

Agreed Action 3.1

Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.

Actions for Schools

1. To provide either a named person or post to be designated officer with responsibility for dealing with FOIs and SARs

Priority	3
Responsible Officer	Children’s Services /School(s) / Head teacher(s)
Timescale	31st July 2017

4 Data Back Up

Issue/Control Weakness	Risk
A number of schools were not sure of the location of their back up data and whether this data could be restored.	Back up data could be lost or not function as required.

Findings

Although all fifteen schools confirmed they had procedures in place to back up their finance and admin data on a regular basis:

- One school confirmed they did not store back-up data in a secure location or away from the main server and one was not sure (the back up being held by the IT managed service contractor).
- Five had not tested (or had not asked their IT managed service contractor to test) that data could be restored from their back-ups.

Agreed Action 4.1

Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.

Priority	2
Responsible Officer	Children’s Services /School(s) / Head teacher(s)
Timescale	31st December 2016

<u>Actions for Schools</u>

1. Check contracts with their IT managed services providers or suppliers where
   a. Back up data is stored
   b. How it is stored
   c. Is it retrievable/able to be restored from back ups
2. If there is no back up and/or inadequate security of back up data and/or no restoration ability, to urgently put these into place and ensure this is evidenced. Ongoing quality checking/monitoring and /or testing should be put in place

5 Disposal of Records

Issue/Control Weakness	Risk
Schools were unable to evidence destruction of records in accordance with document retention schedules.	Failure to comply with Data Protection Principles for retention of records.

Findings

Schools should ensure that records, both physical and electronic, are destroyed in accordance with the schools document retention schedule. Of the fifteen schools returning questionnaires:

- Three schools were not clear how retention guidelines were applied to personal information (such as files for staff and students) and how long personal files should be retained.
- Although schools confirmed they used suitable methods of disposal for physical records most were not clear on the disposal of electronic records.
- There was no record of what groups of documents had been destroyed in compliance with the document retention guidelines.

Agreed Action 5.1

Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.

Priority	3
Responsible Officer	Children’s Services /School(s) / Head teacher(s)
Timescale	31st July 2017

<u>Actions for Schools</u>

1. Introduce or review retention guidance, schedules etc based on legislative/statutory records management and/or best practice including method(s) for recording destruction of information etc
2. Introduce or review current disposal methods for electronic records ensuring they meet information security/Data Protection Act (DPA) etc requirements

6 Encryption

Issue/Control Weakness	Risk
Data held on portable storage devices such as laptops and memory sticks was not adequately protected at all schools and confidential or sensitive information could be accessible by unauthorised persons.	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:

- Five schools had laptops that could be used to hold personal data that were password controlled but not encrypted.
- Four schools used unencrypted memory sticks.

Agreed Action 6.1

Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.

Priority	2
Responsible Officer	Children’s Services /School(s) / Head teacher(s)
Timescale	31st December 2016

Actions for Schools

1. Ensure that all portable storage devices eg laptops, memory sticks etc are encrypted

7 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

Schools need to ensure that data passed to other data controllers and third party providers is transmitted and held securely and is only used in accordance with the schools privacy notice. It was noted that there is no formal data sharing protocol agreement in place at schools which clearly sets out the responsibilities of both parties:

- Six schools did not know whether information sharing protocols were in place to govern routine information sharing with other data controllers.
- Six schools did not know whether there were contracts in place to govern the work of data processors (third party providers) that provide assurance of their compliance with data protection principles.

Agreed Action 7.1

Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.

Priority	3
Responsible Officer	Children's Services /School(s) / Head teacher(s)
Timescale	31st December 2016

<u>Actions for Schools</u>

1. Review what data is shared and with who and for what purpose
2. Put in place or review information sharing agreements
3. Review contracts with data processors to ensure DPA compliance

8 CCTV

Issue/Control Weakness	Risk
Schools may not be compliant with the information Commissioners Code of Practice for the use of CCTV.	Data Protection breaches may occur.

Findings

Nine out of the fifteen schools returning questionnaires had CCTV cameras in place and had specified the use of CCTV on their data registration. However, two schools indicated on the questionnaire that they were unable to confirm that they were compliant with the Information Commissioners code of practice for the use of CCTV and schools did not have their own policy or procedures in place to ensure compliance.

Agreed Action 8.1

Each school is its own data controller and is legally responsible for complying with data protection legislation. The findings from the internal audit report will be shared with all headteachers and will include recommended action points to consider implementing. It will be suggested that all schools consider completing a data protection risk assessment in the first instance. If training and support is required arrangements can be made through the CYC team to provide this through the traded service for Information Governance or alternatively support can be obtained through other organisations.

Priority	3
Responsible Officer	Children’s Services /School(s) / Head teacher(s)
Timescale	31st December 2016

<u>Actions for Schools</u>

1. Introduce as a minimum, the ICOs code of practice on use of CCTV in schools
2. Introduce or review the policy and procedures covering CCTV use in schools

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.