Veritau
Assurance Services for the Public Sector

York High School

City of York Council

Internal Audit Report 2016/17

Business Unit: Children's Services, Education & Skills,
Headteacher: D Ellis
Date Issued: 02/02/17
Status: Final
Reference: 15692/003

	P1	P2	P3
Actions	**0**	**0**	**1**
Overall Audit Opinion	High Assurance		

CITY OF YORK COUNCIL

Summary and Overall Conclusions

Introduction

This audit was carried out on Tuesday 6th December and Wednesday 7th December 2016 as part of the Internal Audit plan for Education, Skills and Children's Services for 2016/17.

Objectives and Scope of the Audit

The purpose of this audit was to provide advice to the Governors, Head Teacher and the Authority's Section 151 Officer about the financial management procedures and assurance that internal controls of the school were operating effectively to manage key risks, both financial and otherwise. The audit covered the following areas in accordance with the specification issued on 21st October 2016:

- Governance;
- Financial Management;
- System Reconciliation;
- Petty Cash
- Contracts – Ordering, Purchasing and Authorisation;
- Income;
- Capital and Property;
- Additional School Activity Provision;
- Human Resources;
- Payroll;
- School Meals;
- Pupil Numbers;
- Voluntary Funds Monitoring Arrangements;
- Data Protection and Information Technology;
- Insurance and Risk Management;
- Joint Use Facilities;
- Inventory Records;
- Minibus;
- Security; and
- Safeguarding Arrangements.

Key Findings

Systems at the school were operating well in all the areas reviewed with only one formal recommendation being made for a procedure to be put in place and notified to staff to cover data breach management. In relation to Information Governance it is also suggested that the school apply an automatic prompt to staff to periodically change initial log on passwords and that there is a review of whether personal data is shared with any external organisations or contractors to ensure information sharing agreements are in place where appropriate.

Overall Conclusions

It was found that the arrangements for managing risk were very good. An effective control environment appears to be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided High Assurance.

1 Information Governance

Issue/Control Weakness	Risk
The school did not have a policy or formal procedure in place that covered data protection breaches.	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

Each school is its own data controller and is legally responsible for complying with data protection legislation. The school has a data security policy in place which is subject to annual review. There is however no documented policy or procedure for managing actual or suspected data breaches where personal or sensitive data may have been compromised, disclosed, copied, transmitted, accessed, lost, stolen or used by unauthorised individuals.

Recommendation

The school should introduce a data breach management policy or procedure which should be notified to all staff. The procedure should include details of how breaches will be reported, investigated and actions to be taken. In the case of serious breaches liaison with the Council's Information Governance Officer is advised and reporting to the Information Commissioner may be required. Advice on policy and procedure has been sent to the school.

Agreed Action 1.1

The policy is being reviewed to include a procedure to follow in the event of a data breach. The policy will be presented to the Governors Staffing, Finance and Premises Committee on 01/03/2017 for approval and ratified at the Full Governing Body meeting on 09/03/2017. Once ratified the policy will be available to staff in the staff handbook.

Priority	3
Responsible Officer	Ian Parnaby
Timescale	Completed by 09/03/2017

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.