APPENDIX D

AMBER REPORTS ISSUED QUARTER 4 2016/17

ARTHOG OUTDOOR EDUCATION CENTRE

1. Introduction and Scope

1.1 An audit review commenced on 24th October 2016, to provide an opinion on the control environment and a level of assurance for Arthog Outdoor Education Centre. The scope of the audit was agreed by the Outdoor Education Manager.

1.2 We would like to thank the following for their help during the audit:

Outdoor Education Manager
Arthog Administrator
ArthogCaterer
ArthogCaretaker

2. Good Practice Areas

2.1 During the audit a good practice area was identified with regard to the booking procedures and processes which are managed well.

3. Management Summary and Overall Opinion

3.1 On the basis of the work carried out, our opinion based on the level of assurance provided by the controls for this audit area is Limited - whilst there is basically a sound system of control, there are weaknesses in the system that leaves some risks not addressed and there is evidence of non-compliance with some key controls.

3.2 Recommendations have been made to strengthen the controls found to require improvement. We have included a risk rating - High, Medium, and Low- for each recommendation to assist you in the prioritisation of their implementation.

Recommendation Risk Rating	Number	Percentage
High	1	3%
Medium	30	94%
Low	1	3%
Total	**32**	**100%**

3.3 As part of the audit process we also identified some minor items that did not require recorded recommendations but were discussed at the closure discussion meeting with the Outdoor Education Manager.

3.4 As part of this audit we have also followed up the implementation of recommendations made in the previous audit report dated 12th March 2013. The table below shows the action taken since that audit:

Recommendation Category	Implemented	Not Implemented so reiterated in this audit	Agreed future Implementation
Legal Requirement	1		
Financial Regulation	16	5	
Policy/Procedure	16	5	

Best Practice			
Total	**33**	**10**	

3.5 The implementation of the recommendations made in this report and those outstanding from the previous review will further strengthen the controls and processes at Arthog Outdoor Education Centre.

ADDITIONAL PAYMENTS TO FOSTER CARERS

1. Introduction and Scope

1.1 An audit review commenced in November 2016, to provide an opinion on the risk and control environment and a level of assurance for Additional Payments to Foster Carers. The scope of the audit was agreed by Service Delivery Manager Family Placements, Children in Care, Leaving Care & EDT.

1.2 We would like to thank the following for their help during the audit:

- Service Delivery Manager Family Placements, Children in Care, Leaving Care & EDT
- Senior Social Worker
- Support Services Team leader
- Support Services Officer - Finance

2. Management Summary and Overall Opinion

2.1 On the basis of the work carried out, our opinion based on the level of assurance provided by the controls managing the risks for this audit area is **Limited.** Whilst there is basically a sound system of control, there are weaknesses in the system that leaves some risks not addressed and there is evidence of non-compliance with some key controls.

2.2 Recommendations have been made to strengthen the controls found to require improvement. We have included a risk rating - High, Medium, and Low- for each recommendation to assist you in the prioritisation of their implementation.

Recommendation Risk Rating	Number	Percentage
High	4	17%
Medium	16	70%
Low	3	13%
Total	**23**	**100%**

2.3 The implementation of the recommendations made in this report will further strengthen the controls, management of risks and processes in the Additional Payments to Foster Carers process.

TEAGUES BRIDGE PRIMARY SCHOOL

1. Introduction and Scope

1.1 An audit review was commenced on 26th September 2016, to provide an opinion on the control environment and a level of assurance for Teagues Bridge Primary School.

1.2 We would like to thank the following for their help during the audit:
Headteacher

School Business Manager
Administrative Assistant

2. Management Summary and Overall Opinion

2.1 On the basis of the work carried out, our opinion based on the level of assurance provided by the controls for this audit area is Limited. Whilst there is basically a sound system of control, there are weaknesses in the system that leaves some risks not addressed and there is evidence of non-compliance with some key controls.

2.2 Recommendations have been made to strengthen the controls found to require improvement. We have included a risk rating - High, Medium, and Low- for each recommendation to assist you in the prioritisation of their implementation.

Recommendation Risk Rating	Number	Percentage
High	5	25%
Medium	11	55%
Low	4	20%
Total	**20**	**100%**

2.3 As part of the audit process we also identified some minor items that did not require recorded recommendations but were discussed at the closure discussion meeting with the Headteacher and School Business Manager.

2.4 As part of this audit we have also followed up the implementation of recommendations made in the previous audit. The table below shows the action taken since that audit:

Recommendation Category	Implemented	Not Implemented Recommendation Reiterated
Legal Requirement	1	-
Financial Regulation	5	3
Policy/Procedure	6	1
Best Practice	1	1
Total	**13**	**5**

2.5 The implementation of the recommendations made in this report and those outstanding from the previous review will further strengthen the controls and processes at Teagues Bridge Primary School.

ICT - ANTI VIRUS/MALWARE ARRANGEMENTS

1. Introduction and Scope

1.1 An audit review was commenced on 27th September 2016, to provide an opinion on the control environment and a level of assurance for Anti-Virus/Malware arrangements. The scope of the audit was agreed by ICT Education Services Architect. It should be noted that security scanning of the anti-virus hosts has not been undertaken as part of this audit as security scanning will form part of the Network Management review which is also being undertaken in 2016/17

1.2 We would like to thank the following for their help during the audit:

SCCM & Deployment Specialist – ICT

Business Support Supervisor - ICT

2. Good Practice Areas

2.1 During the audit a number of good practice areas within the process for Anti-virus / Malware Arrangements were identified. These included:

- End user security training arrangements are in place;
- A defence in depth approach is taken to network perimeter security.
- Anti-virus definitions are regularly updated and distributed;
- There are both default and specific anti-virus software policies in place;
- The anti-virus solution provides access to a central management console;
- A general incident response procedure is in place.

3. Management Summary and Overall Opinion

3.1 On the basis of the work carried out, our opinion based on the level of assurance provided by the controls for this audit area is **Limited** - *Whilst there is basically a sound system of control, there are weaknesses in the system that leaves some risks not addressed and there is evidence of non-compliance with some key controls*

3.2 Malicious software (malware) has become increasingly more evolved and sophisticated and as such poses an increasing threat to all organisations. Software and hardware technologies for helping to prevent malware threats and attacks have also increased in their complexity and sophistication and this includes anti-virus software. Whilst organisations cannot rely solely on anti-virus software for its malware defences it nevertheless remains one of the prime forms of protection from malicious software attacks. The Council has deployed anti-virus software as part of its overall cyber defence mechanisms. Although there were areas of good practice such as the development of specific anti-virus software policies rather than simply reliance on generic policies there were weaknesses identified in control processes which have impacted significantly on the opinion formed.

3.3 Recommendations have been made to strengthen the controls found to require improvement. We have included a risk rating - High, Medium, and Low- for each recommendation to assist you in the prioritisation of their implementation.

Recommendation Risk Rating	Number	Percentage
High		
Medium	10	83%
Low	2	17%
Total	**12**	**100%**

3.4 The implementation of the recommendations made in this report will further strengthen the controls and processes in respect to anti-virus/malware arrangements.

ICT – CONTROL OF PRIVILEGED USERS INCLUDING THE USE & SUPPORT OF ADMINISTRATION TOOLS

1. Introduction and Scope

1.1 An audit review was commenced on 1st November 2016, to provide an opinion on the control environment and a level of assurance for the control of privileged users including the use and support of administrative tools. The scope of the audit was agreed by ICT Education Services Architect.

1.2 We would like to thank the following for their help during the audit:

ICT Education Services Architect
ICT Infrastructure Specialist
Cloud and Mobile Systems Specialist
SCCM & Deployment Specialist – ICT
Network & Solutions Architect

2. Good Practice Areas

2.1 During the audit a number of good practice areas within the process for the control of privileged users including the use and support of administrative tools were identified. These included:

- There is general policy that administrators login to their own unique accounts with administrative rights only when necessary to perform actions requiring those rights.
- Access to privileged workstations is restricted through the application of Active Directory and network policies.
- Access for all users including privileged access is logged through Change Auditor.
- Critical events including changes to privileged Active Directory groups are issued as e-mail alerts.

3. Management Summary and Overall Opinion

3.1 On the basis of the work carried out, our opinion based on the level of assurance provided by the controls for this audit area is **Limited** - w*hilst there is basically a sound system of control, there are weaknesses in the system that leaves some risks not addressed and there is evidence of non-compliance with some key controls.*

3.2 The SANS Institute, an organisation specialising in publishing guidance and training in information security and cybersecurity, routinely publishes a list of the top 20 Critical Security Controls for Effective Cyber Defence. These critical controls include the controlled use of administrative privileges and the inventory of authorised and unauthorised software. Threats to the security of an organisation evolve and new ones emerge on a daily basis, however the misuse of administrative privileges continues to be a primary method for attackers to spread inside a target enterprise, similarly attacks based on scanning target organisations looking for vulnerable versions of software that can be exploited also remains a consistent method of attack. Although there were areas of good practice there were weaknesses identified in control processes which have impacted significantly on the opinion formed.

3.3 Recommendations have been made to strengthen the controls found to require improvement. We have included a risk rating - High, Medium, and Low- for each recommendation to assist you in the prioritisation of their implementation.

Recommendation Risk Rating	Number	Percentage
High		

Medium	7	54%
Low	6	46%
Total	**13**	**100%**

3.4 The implementation of the recommendations made in this report will further strengthen the controls and processes in the control of privileged users and the use and support of administrative tools.