APPENDIX D

ABACUS SYSTEM REVIEW

1. Introduction and Scope

1.1 An audit review was undertaken between March – June 2011, to provide an opinion on the control environment and a level of assurance for the administration of the Abacus System.

1.2 The scope of the audit was agreed by the Team Leader ICT Application Support and the Assessment & Welfare Team Leader (Finance).

1.3 There was a delay in issuing the report due to the availability of key staff and the finance restructure.

2. Management Summary and Overall Opinion

2.1 This audit has highlighted some major concerns with the Abacus system, specifically around the following:

a) Clarity of ownership of the system and general roles and responsibility. Key officers in respect to Abacus are due to leave the authority soon so their roles and responsibilities need to be defined and then re-assigned.
b) Authorisation – there are currently no formal authorisation limits for the Abacus system.
c) Abacus does not distinguish between Children's and Adult records and as such the system could allow an officer to access or authorise a transaction relating to either service.
d) Information Governance (IG) has been consulted with on an adhoc basis with regard to the development of the system. Given the nature of information being processed it seems likely that there may be data protection and data security implications therefore IG should have been more formally involved with the project from the outset.

2.2 Out of the 63 controls reviewed during this audit, 36 (57%) were found to be satisfactory. On the basis of the work carried out it is our opinion that the level of assurance provided by 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. There are a number of legal and/or financial regulation recommendations or recommendations concerning areas of high priority to the Council. The grading of this report was agreed as Amber during the discussions of the draft report.

2.3 Recommendations have been made to improve the controls found to be unsatisfactory and these are categorised as shown below.

Recommendation Category & timescale	Number	Percentage
Legal Requirement – immediate implementation	3	15%
Financial Regulation – immediate implementation	2	10%
Policy/Procedure – implementation within a month of agreement to the report.	14	70%
Best Practice – implementation at a mutually agreed date	1	5%
Total	**20**	**100%**

2.4 The implementation of the recommendations made in this report will further strengthen the controls and processes in your area.

IT BACK UP AND RECOVERY

1. Introduction and Scope

1.1 An internal audit was undertaken in April 2011, to provide an opinion on the control environment and a level of assurance on the adequacy of the controls in place to manage risks associated with Corporate ICT backup and recovery arrangements.

1.2 The scope of the audit was agreed by the ICT Service Delivery Manager and the Infrastructure Development and Support Team Leader (who has since left the Council).

2. Good Practice Areas

2.1 During the internal audit, a number of good practice areas within the arrangements for Backup & Recovery were identified. These included:

- A Business impact analysis has been carried out with each Service Delivery Team to determine the critical functions, locations and systems within the Council.
- Critical functions and systems have been prioritised for recovery, and recovery time objectives have been set per priority.
- It is acknowledged that rigorous efforts are being made to implement the disaster recovery arrangement as part of the Infrastructure Project.
- Council systems are backed up on a periodic basis and errors in back up are investigated.
- Weekly and monthly backup tapes stored at Granville House are stored in a secure fireproof environment.

3. Management Summary and Overall Opinion

3.1 Out of the 21 controls tested, (15%) were found to be satisfactory. On the basis of the work carried out, it is our opinion that the level of assurance provided by 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) and the key weaknesses contributing to this opinion are highlighted in 3.3 and 3.4 below. The grading of this report was discussed and agreed with the Infrastructure Development and Support Team Leader as amber during the discussions of the draft report.

3.2 Recommendations have been made to improve the controls found to be unsatisfactory and these are categorised as shown below:

Recommendation Category & timescale	Number	Percentage
Legal Requirement – immediate implementation	2	20%
Financial Regulation – immediate implementation	-	-
Policy/Procedure – implementation within a month of agreement to the report.	8	80%
Best Practice – implementation at a mutually agreed date	-	-
Total	**10**	**100%**

3.3 One of the main weaknesses of current arrangements is a lack of a documented disaster recovery plan which is pending due to the ongoing implementation of disaster recovery arrangements.

3.4 Disaster recovery arrangements involve the virtualisation of all the physical servers within the Council where possible. These servers and the data would then be replicated to another site which would be the disaster recovery hot site to recover all virtual servers. Currently this does not exist and reliance is placed on best endeavours and ability to restore from back-ups to provide recovery for any services during a disaster.

3.5 Audit testing of the backup and disaster recovery arrangements were only carried out for the corporate environment. Backup and disaster recovery arrangements provided by the Council for Education Services was outside the scope of this audit.