AGS 2016/17 Action Plan Review

Issue Identified	Source of Evidence	Update/Summary of Action Taken & Proposed	By whom & By when	Current Position
Information Governance and breaches in Data Protection are not adequately managed.	Internal Audit Report	Plans are now in place to: • Assign clear roles and responsibilities; • Approve and implement the necessary policies and procedures; • Deliver a targeted training programme; • Ensure adequate reporting arrangements; and • Consider appropriate disciplinary procedures for data breaches. Internal Audit to assist/advise.	Solicitor to the Council 31 December 2017 Amended deadline	Actions implemented - A high level action plan was included as part of the Information Governance Annual Report 2015/16 presented to Audit and Governance Committee in January 2016. In October 2016 Veritau reported in relation to Information Governance and Freedom of Information and gave an opinion of reasonable assurance, finding that the Council has made significant progress since previous audit but some weaknesses remain. On-going actions are monitored by the Audit and Governance Committee through the Annual Information Governance report.

AGS 2016/17 Action Plan Review

Issue Identified	Source of Evidence	Update/Summary of Action Taken & Proposed	By whom & By when	Current Position
Non-compliance with the Payment Card Industry Data Security Standard (PCI DSS)	Internal Audit report	Agreed actions: • Management responsibility has been defined • The cardholder data environment will be mapped and documented • Policies and procedures will be developed in relation to PCI DSS • Dependencies on third parties will be explored and assessed • Responsibility for completing annual self-assessment questionnaires will be assigned Internal Audit to assist/advise. Regular updates will be brought to the Audit and Governance Committee during 2017/18.	Lead Officer Data and Systems 31 March 2018 Amended deadline	Discussions ongoing with the service provider re: the financial and technical viability of setting up a 'hosted payment page' on the website – to eliminate card processing and storage on the Council's network. Contact Centre computers updated to support PCI DSS compliance for payments made by customers in the CCC. Operational/compliance procedure notes drafted for internal payment processing. This will be appended to the revised Data Protection Policy (being revised to account for GDPR).
A further review of ICT disaster recovery arrangements has been	Internal Audit report	Arrangements for Disaster Recovery transferred from Craven	Head of Business Development.	Action plan in place to address the issues identified, e.g. arrangement with NYCC

AGS 2016/17 Action Plan Review

Issue Identified	Source of Evidence	Update/Summary of Action Taken & Proposed	By whom & By when	Current Position
undertaken in 2015/16 – further actions have been identified: A new ICT Disaster recovery Plan will be developed which will include responsibilities (and responsible officers), invocation procedures and responsibilities for actions The new ICT Disaster Recovery Plan will include provision for a number of system restoration tests over the period of agreement. A programme of back-up tests will be put in place and encryption of tapes will be investigated. New arrangements for data and systems replication will be put in		DC to North Yorkshire CC at the end of April 2017. An overarching disaster recovery plan has been approved. The plan details roles and responsibilities across SDC, NYCC and other partners. A plan to secure even greater resilience is being developed in conjunction with NYCC. Implementation of this will run through 2017/18 and beyond. Plans are in place to test DR arrangements throughout the year. A framework for prioritising which systems are restored first. has been developed. A review of Business Continuity Planning in late summer/early autumn will re-	All actions will be completed by 31 Dec 2017. Amended deadline	has allowed rationalisation of back-up contracts. £50k bid to support work on addressing DR risks included in draft budget for 2018/19. If approved, priorities will include updating remote access and modernising our back-up solution. Working with NYCC to sign up to GovRoam which will support staff to access SDC networks via NYCC and other public sector wifi networks. Revised Business Continuity Policy agreed by Leadership Team December 2017. Workshop with all Heads of Service to update BCPs scheduled for 11 January 2018 – this will re-affirm details of replacement premises, equipment etc. and

AGS 2016/17 Action Plan Review

Issue Identified	Source of Evidence	Update/Summary of Action Taken & Proposed	By whom & By when	Current Position
place with NYCC.		affirm details of replacement premises, equipment etc. this will then support more detailed testing.		support detailed testing of DR arrangements. Note: DR work is ongoing – and will continue to be so but for the purposes of this update the actions have been completed.
Creditors (Raised 2016/17)	Internal Audit report	A number of duplicate invoices and payments were identified during the audit. In addition, a high number of orders were found to be raised outside of the e-procurement system.

An action plan was agreed and good progress has been made towards this with an update provided to the Audit and Governance Committee in April 2017. | Head of Operational Services

30 June 2017 | Actions have been implemented. Creditors has been included in the audit plan for 2017/18 and a follow-up of the issues identified will be carried out. |

AGS 2016/17 Action Plan Review

Issue Identified	Source of Evidence	Update/Summary of Action Taken & Proposed	By whom & By when	Current Position
Payroll reconciliation (Raised 2016/17)	Internal and External Audit reports	Delays to and errors within with the payroll costing file	Head of Finance 30 June 2017	Ongoing issues have been escalated within NYCC and the issues have now been fully resolved.