REPORT TO:	**FINANCE AND MANAGEMENT COMMITTEE**	**AGENDA ITEM: 9**
DATE OF MEETING:	**26th APRIL 2012**	**CATEGORY: RECOMMENDED**
REPORT FROM:	**CHIEF EXECUTIVE OFFICER**	**OPEN**
MEMBERS' CONTACT POINT:	**KEVIN STACKHOUSE (01283 595811) HEAD OF CORPORATE SERVICES** Kevin.stackhouse@south-derbys.gov.uk	**DOC:** u/ks/corporate plan & constitution/security policies
SUBJECT:	**UPDATE OF SECURITY and FRAUD POLICIES**	**REF**
WARD (S) AFFECTED:	**ALL**	**TERMS OF REFERENCE: FM 03**

1.0 Recommendations

1.1 That the relevant amendments to the Constitution as detailed in the report are approved.

2.0 Purpose of Report

2.1 To update the Constitution in the areas that deal with financial procedures and security in respect of procurement, fraud and corruption. In particular, the following policies require updating:

- ICT Security Policy and Procedures
- Debit/Credit Card Security Policy and Procedures
- Anti-Fraud and Corruption Policy

2.2 The report summarises the changes to these policies with the full policies being available on the Council's Intranet. Links are provided at the end of this report.

3.0 Detail

Current Position

3.1 Part 4 of the Constitution sets out the detailed arrangements in respect of Risk Management, particularly with regard to fraud and corruption, together with systems integrity and security.

3.2 With recent changes in legislation such as the Bribery Act 2010, together with the manner in which greater elements of the Council's business around procurement and payment for goods and services is now conducted electronically and "on-line," it is considered that a number of variations to existing policies and procedures are necessary to bring the Constitution up to date.

Proposed changes

3.3 The associated policies and procedures have been in place for up to 3 years but now require updating.

3.4 The policies are very procedural and operational in nature. They are designed to protect and safeguard the Council from potential security breaches and fraudulent acts. They also act as procedural guides to employees to ensure that they act properly in relation to on-line transactions and in making card payments on behalf of the Council.

ICT Security Policy and Procedures

3.5 The Council is dependent upon Information Technology for its normal day to day business activities. It is therefore essential for the successful operation of the Council that the confidentiality, integrity and availability of its IT systems and data are maintained at a high level.

3.6 There is also an obligation on the Council and all employees to comply with relevant legislation such as the Data Protection Acts, the Copyright, Designs & Patents Act and the Misuse of Computers Act. It follows that a high standard of IT security is required within the Council.

3.7 The Policy describes how IT Security is dealt with at the Council and the measures that have been introduced to prevent security breaches. The purpose of the Policy is to preserve:

- **Confidentiality -** Access to data is confined to those specifically authorised to view it.
- **Integrity -** Data is up to date and accurate, and is deleted or amended only by those authorised to do so.
- **Availability -** Data is available to those authorised when it is needed.

3.8 Having reviewed this policy, the only changes required are in terminology and to reflect the relationship with Northgate as the Council's IT service provider.

Credit/Debit Card Security Policy and Procedures

3.9 This document sets out the policy and procedures for:

- Handling credit/debit card payments received by the Council
- Dealing with payments to suppliers for services to the Council
- Overall security and related matters

3.10 It describes how both credit/debit card transactions and security is handled together with the measures necessary to prevent security breaches.

3.11 Some terminology changes have been made and a separate section added on using cards specifically for purchases. It also reflects the relationship with suppliers.

Anti-Fraud and Corruption Policy

3.12 The purpose of this Policy is to set out responsibilities regarding the prevention of fraud, error and corruption, together with procedures to be followed where a fraud, error or corruption is suspected or detected.

3.13 It applies to Members, employees, together with the principals and employee's of commercial organisations contracted to undertake work on behalf of the Authority. This includes agency workers, consultants, suppliers and organisations funded by the Council.

3.14 The Policy is intended to be as comprehensive as possible. However, in the absence of an issue or an act which could be considered to be fraudulent or corrupt, its absence from this policy document does not invalidate it.

3.15 The objective of the Policy is to promote the prevention of fraud and corruption, the detection and investigation of suspected fraud and corruption, to deter fraud and corruption and to take appropriate and decisive action against any attempted or actual fraudulent or corrupt activity affecting the Council.

3.16 In order for the Council to be effective in its approach to dealing with the problem of fraud and corruption, it is important that it creates a culture of intolerance rather than indifference to such matters. The Policy also seeks to draw attention to the prevention or detection of error, which may detrimentally affect the Council both financially and from a reputation point of view.

Bribery Act 2010

3.17 This Policy has been updated mainly to reflect the requirements of the Bribery Act 2010. This Act makes it a criminal offence to give a bribe in order to induce or reward an individual for the improper performance of a relevant function or activity.

3.18 It also provides a criminal offence for an individual to request or agree to receive a bribe for the improper performance of a relevant function or activity.

The Council's Responsibility

3.19 The Act also provides a corporate offence of failing to prevent bribery. Although an organisation cannot ultimately prevent a deliberate act, it must do all it reasonably can to mitigate any occurances. Consequently, it must have robust policies and procedures in place to strengthen control, provide guidance, assess risk and promote a culture of non-tolerance.

3.20 As with the other policies, some terminology and legislative references have been changed and there are now specific links to the Whistle Blowing and Anti Money Laundering Policies of the Council as these may have fraudulent implications. In addition the following changes have been made.

- To reflect the requirement for managers to check that employees are eligible to work in the UK.

- Information on the use of Counter Fraud Intelligence

- Fraud response procedure for staff

- A fraud prosecution policy has been added.

4.0 Financial Implications

4.1 None

5.0 Corporate Implications

5.1 The revised anti fraud, corruption and security arrangements will impact on individual staff and managers' responsibilities.

5.2 Therefore, it is timely for briefing sessions will be held for designated staff and managers to raise awareness to ensure that potential risks to the Council are minimised. The briefings will also facilitate a cascade of information throughout the organisation.

5.3 In addition, it is also recommended that awareness is raised amongst Members.

6.0 Community Implications

6.1 None directly

7.0 Background Papers

7.1 The full and updated policies are available at:

ICT Security

http://harvey/corporate/ITServices/folder.2005-11-08.1583282127/

Credit/Debit Card Security

http://harvey/corporate/ITServices/folder.2005-11-08.1583282127/ccsecurityprocs/ccsecuritypolicyprocedure/view?portal_status_message=Your%20changes%20have%20been%20saved

Anti Fraud and Corruption

http://harvey/corporate/anti_fraud_corruption_policy/view?portal_status_message=Your%20changes%20have%20been%20saved.