ABERDEEN CITY COUNCIL

COMMITTEE	Finance Policy & Resources
DATE	1st December 2017
REPORT TITLE	Protective Monitoring
REPORT NUMBER	CG/17/121
CG LEAD OFFICER	Steven Whyte
REPORT AUTHOR	Norman Hogg

1. PURPOSE OF REPORT:-

1.1 To provide assurance that Protective Monitoring is performed in line with legislation and best practice.

2. RECOMMENDATION(S)

2.1 That the committee note, review and agree the following documents, attached as appendices, which make up the suite, 'Protective Monitoring':

Protective Monitoring Policy
Protective Monitoring Privacy Impact Assessment
Protective Monitoring Risk Assessment
Protective Monitoring Human Rights Impact Assessment
Protective Monitoring Access to Information Procedure
Access to Information Guide and Form

3. BACKGROUND/MAIN ISSUES / OTHER HEADINGS AS APPROPRIATE

3.1 Protective Monitoring (using event data to identify potential security issues) within ICT is an essential requirement. To not exercise protective monitoring would put the council at extreme risk, would find the council falling foul of the Data Protection Act, be against best practice and be negligent in their duty of care.

3.2 Monitoring however must be a balance between protecting the business and the individual while at the same time respecting the rights of those individuals under such legislation as the Human Rights Act 1998

3.3 The documents created and supplied for review:

- Identify why, what and how we monitor.
- Demonstrate that we have thought about this (due diligence).

- Demonstrates that we have processes in place.
- Demonstrates that protective monitoring protects both the business and the individual.

3.4 The council is on a programme of digital transformation and the Government state a Cloud First policy. This by its nature shifts the boundary of the network and it becomes even more important to implement sound protective monitoring strategies within the organisation.

4. FINANCIAL IMPLICATIONS

4.1 There are no financial implications.

5. LEGAL IMPLICATIONS

5.1 The suite of documents has been passed to Legal and Democratic Services for Review.

5.2 Various Acts are referenced in the suite of documents and listed here in Summary:

5.3 Acts

- The Data Protection Act 1998
- General Data Protection Regulation
- The Computer Misuse Act 1990
- The Copyright, Designs and Patents Act 1988
- The Health & Safety at Work Act 1974
- The Human Rights Act 1998
- The Regulation of Investigatory Powers (Scotland) Act 2000
- Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000 (LBPR).

5.4 Standards

- ISO27001/2 (Information Security standards)
- PSN (Public Services Network standards)

5.5 Regulations

- PCI DSS (Payment Card Industry Data Security Standard)

5.6 Best Practice Guides

- National Cyber Security Centre (NCSC) Good Practice Guide 13 - Protective Monitoring (GPG 13)
- Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work.

6. MANAGEMENT OF RISK

Financial

6.1 There are no financial risks to the Council in agreeing these recommendations.

Employee

6.2 By agreeing the recommendations risks are minimised for the employee due to policy, procedure and supporting material being documented and communicated.

Risk - Low

Customer / Citizen

6.3 There are no risks to the customer / citizen in agreeing these recommendations.

Environmental

6.4 There are no environmental risks in agreeing these recommendations.

Technological

6.5 There are no technological risks in agreeing these recommendations.

Legal

6.6 By agreeing the recommendations legal risks are minimised due to evidence of due diligence and consideration of the listed acts and regulations.

Risk - Low

Reputational

6.7 There are no reputational risks to the Council in agreeing these recommendations.

Other

6.8 The document 'Protective Monitoring Risk Assessment' further highlights the risks to the business and to the individual in performing or not performing protective monitoring.

7. IMPACT SECTION

7.1 Economy

7.1.1 Protective Monitoring is one aspect of securing the customer data entrusted to us and has a positive impact on the local economy. Securing customer data underpins the digital aspects of the local economy.

7.2 People

7.2.1 Protective Monitoring is one aspect of securing the customer data entrusted to us and therefore has a positive impact for our customer.

7.3 Place

7.3.1 Protective Monitoring is one aspect of securing the customer data entrusted to us. All customers including investors and visitors to the City expect their data to be appropriately secured.

7.4 Technology

7.4.1 Implementing and extending protective monitoring as new technology is introduced is essential in ensuring security is maintained as per best practice.

8. BACKGROUND PAPERS

8.1 Various documents are referenced within the appendices and listed here in Summary:

8.2 Standards

- ISO27001/2
- PSN

8.3 Regulations

- PCI DSS

8.4 Best Practice Guides

- National Cyber Security Centre (NCSC) Good Practice Guide 13 - Protective Monitoring (GPG 13)
- Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work.

9. APPENDICES (if applicable)

CG.17.121 - Appdx 1 Protective Monitoring Policy
GC.17.121 - Appdx 2 Privacy Impact Assessment
CG.17.121 - Appdx 3 Risk Assessment
CG.17.121 - Appdx 4 Access to Information Procedure
CG.17.121 - Appdx 5 Access to Information Guide and Form

10. REPORT AUTHOR DETAILS

Norman Hogg
Security Architect
nohogg@aberdeencity.gov.uk
01224522407

HEAD OF SERVICE DETAILS

Simon Haston
Head of IT & Transformation
shaston@aberdeencity.gov.uk
07768725244