ABERDEEN CITY COUNCIL

COMMITTEE	Audit Risk & Scrutiny
DATE	8th May 2018
REPORT TITLE	Protective Monitoring
REPORT NUMBER	CUS/18/007
DIRECTOR	Andy MacDonald
REPORT AUTHOR	Norman Hogg
TERMS OF REFERENCE	1.4

1. PURPOSE OF REPORT

1.1 To provide assurance that Protective Monitoring is performed in line with legislation and best practice and provide further update on the governance process for officers and elected members.

2. RECOMMENDATION(S)

That the Committee: -

2.1 Approves the following documents, attached as appendices, which make up the suite, 'Protective Monitoring':

a) Protective Monitoring Policy
b) Protective Monitoring Privacy Impact Assessment
c) Protective Monitoring Risk Assessment
d) Protective Monitoring Access to Information Procedure
e) Access to Information Guide and Form

3. BACKGROUND

3.1 A report on Protective Monitoring was previously submitted for approval to the meeting of the Finance Policy & Resources Committee held on Wednesday 6th December 2017.

3.2 The Committee resolved:

(i) To defer deliberation of the report until a future meeting of the Committee;
(ii) To instruct officers to include further details within the report regarding the governance process for officers and elected members;

(iii) That officers circulate further details in relation to Airwatch regarding due process;
(iv) That members contact the Head of IT and Transformation with any additional governance and assurance issues that they would like to be addressed and included within the report.

3.3 As the Finance, Policy and Resources Committee has been disestablished, the update under action (ii) is presented to the Audit Risk & Scrutiny Committee in terms of section 1.4 of the terms of reference for the Audit, Risk and Scrutiny Committee.

3.4 Action (iii) has been completed and information was collated and sent in December to Councillor Reynolds by Steven Robertson (Infrastructure Architect). In terms of action (iv), no additional issues were raised by members.

3.5 Protective monitoring is an essential part of cyber security practice. The adoption and implementation of a Protective Monitoring policy is a key requirement of the Council's compliance with Public Service Network (PSN) requirements. If the Council does not have an adequate policy in place, there is a real risk that the Council will not be able to use the PSN and therefore would not be able to deliver its functions.

3.6 Information (or data) is one of the Council's most important assets, and it is vital that the Council adequately protects this asset. Protective Monitoring detects and prevents security incidents and alerts the Council to incidents that require further investigation.

Data protection legislation requires the Council to protect the personal data it processes in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The adoption and implementation of this Protective Monitoring Policy would be a key component of evidencing compliance with this requirement. The General Data Protection Regulation, enforceable from 25 May 2018, increases the potential monetary penalties in relation to non-compliance with data protection law from £500,000 to €20 million.

3.7 Monitoring must, however, be a balance between protecting the Council and the individual, whilst at the same time respecting the rights of those individuals under such legislation as the Human Rights Act 1998, and data protection legislation. Therefore, the Access to Information Procedure (see Appendix 4) and Access to Information Guide and Form (see Appendix 5) will ensure that any access to individual accounts is carried out in a way which balances these rights with the needs of the Council, and complies with these laws

3.8 The documents created and supplied for review:

- identify why, what and how the Council monitors data;
- demonstrates that the Council has taken a holistic approach in their duty to due diligence;
- demonstrates that the Council has processes in place; and
- demonstrates that protective monitoring protects both the business and the individual.

3.9 The Council is on a programme of digital transformation and the Government emphasise a Cloud First Policy (https://www.gov.uk/guidance/government-cloud-first-policy) which, by their nature shifts the boundaries of the network and it becomes even more important to implement sound protective monitoring strategies within the organisation.

3.10 All staff and elected members have relevant codes of conduct. The Staff Code of Conduct at 7.4 requires that all staff comply with the ICT Acceptable Use Policy. Section 3.16 of the Councillors Code of Conduct, in regard to use of Council facilities, requires elected members to use Council facilities in accordance with the Council's information technology policies.

3.11 Staff, agency workers, elected members, contractors, sub-contractors, and any person who uses or requires access to the Aberdeen City Council Information Technology, Data Assets or associated Infrastructure must comply with the Corporate ICT Acceptable Use Policy . Of particular relevance are items 4.8 and 4.10 of the policy:

4.8 Monitoring

The Council seeks to safeguard Users of its ICT equipment, systems and networks from inappropriate activities and unacceptable material. One of its safeguards is monitoring, others include a suite of defensive measures at the perimeter and within the network. All Council ICT equipment, systems and networks may be monitored for compliance with current legislation and Council policies. Monitoring also has the following purposes:

- *to establish compliance with Council policies;*
- *to investigate any suspected or actual breaches of Council policy;*
- *to investigate system performance;*
- *to gather evidence for investigative or disciplinary purposes; and*
- *for other legal and security purposes.*

Monitoring is undertaken in accordance with the Council's approved Electronic Monitoring of Use Impact Assessment.

4.10 Consequences of Misuse

The Council may, at its sole discretion, suspend or terminate ICT access, withdraw or remove any material uploaded by the User in contravention of this Policy. The Council may take such action as it considers necessary, including taking disciplinary action or disclosing information to law enforcement agencies.

Any other Users that are not employed by the Council and not subject to the Council disciplinary procedure will be subject to provisions in the contract held with them or other acceptable use agreement they have entered into. In any event misuse may result in the withdrawal of ICT access or equipment, legal action or involvement of law enforcement agencies.

Users should be aware that use of Council ICT equipment, systems and networks may be monitored at all times and monitoring information is retained and used for both routine monitoring reports and to support potential misuse reports.

Authorised Release of Account Information

3.12 In order to protect the individual, whether employees, elected members or others, a two-step authorisation process is proposed before the release of any information in regard to an individual account is granted. This is to ensure that the request for release is legally competent in line with requirements under data protection legislation and that processing is lawful and fair. Information will only be released to the requester if the request is deemed to be lawful, justified, proportionate and necessary.

3.13 The authorities for sign off for release of relevant information to a legitimate requester, for information regarding a Council Employee account, is proposed as follows:

- Manager, Chief Officer (optionally the Senior Information Risk Officer (SIRO) or Chief Executive) **and** Human Resources.

3.14 The authorities for sign off for release of relevant information to a legitimate requester, for information regarding elected members and other non-council employed user accounts, is proposed as follows:

The SIRO (currently the Chief Officer - Governance) **and** the Chief Executive.

3.15 The document ‘Access to Information Procedure’ has been amended appropriately. If the Council agree with the Procedure, this will grant authority to the officers identified in 3.12 and 3.13 to authorise the release of specified information in relation to an account, as long as this is done lawfully in accordance with data protection legislation and the Human Rights Act 1998.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 A robust Protective Monitoring process is required so that the Council can meet several legal obligations. Without robust and fair Protective Monitoring, the Council would likely breach several obligations under various pieces of legislation. The proposed suite of Protective Monitoring documents is deemed to be proportionate, fair, robust and lawfully compliant.

5.2 The Data Protection Act 1998 requires that processing of personal data is done so lawfully and fairly, is used for limited specifically stated purposes and used in way that is adequate, relevant and not excessive. It also imposes a duty on the Council to maintain appropriate security measures to protect personal data.

5.3 The General Data Protection Regulation which replaces the 1998 Act from 25th May 2018, requires the Council to process personal data lawfully, fairly and transparently, and requires the Council to secure the personal data it holds. The GDPR is designed to enable individuals to better control their personal data. Penalties for breaches are more severe than under the 1998 Act.

5.4 The Computer Misuse Act 1990 which disallows unauthorised access or acts in relation to computer systems, data or materials. Protective monitoring helps identify and block such attempts and provides evidential audit trails which can exonerate or provide nonrepudiation.

5.5 The Copyright, Designs and Patents Act 1988 protects the rights of creators to control the ways in which their materials are used. There is a duty on the Council to prevent breaches of Copyright. Elements of Copyright infringement can be identified and prevented through protective monitoring.

5.6 The Health & Safety at Work etc. Act 1974, the Council is obliged to protect the health, including mental health of their employees. Protective Monitoring reduces the stress to employees by shielding them from unwanted or inappropriate material and preventing unintentional actions and their associated consequences.

5.7 Article 8 of the Human Rights Act 1998 is the right to respect for family and private life, home and correspondence. This right is not absolute and must be balanced with the need of the Council to protect its information. Therefore, the Council must carefully consider requests for access to peoples' correspondence to ensure that the need to do so outweighs the need to protect an an individual's human rights.

5.8 The Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000 (LBPR) allow interception of communications by businesses on their own telecommunications networks, for instance, to detect employee-mail abuse or to record telephone conversations to evidence transactions.

5.9 Standards

- ISO27001/2 (Information Security standards) - a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes. Complying with these standards is industry best practice.

- The Council is obliged to have a Protective Monitoring Policy in place, in order to satisfy strict requirements required by the PSN (Public Services Network). The PSN is a shared information and communications infrastructure, and joins up organisations, departments, Authorities, and agencies that deliver public services, whether national, regional, or local. To provide PSN services, suppliers must meet agreed standards of security, technical performance, service management, and governance. Organisations using PSN must also be PSN-compliant. This compliance ensures seamless, and painless, interconnectivity. Without access to the PSN, the Council would not be able to effectively deliver its functions.

5.10 Regulations

PCI DSS (Payment Card Industry Data Security Standard) – The Council is required to meet this standard in order to take card payments. Requirements include to maintain a firewall to protect cardholder data, protect systems against malware and to track and monitor all access to network resources and cardholder data.

5.11 Best Practice Guides

- National Cyber Security Centre (NCSC) Good Practice Guide 13 - Protective Monitoring (GPG 13) which provides advice on good practice to help meet Protective Monitoring obligations.

- The Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work. (https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf) is intended to help employers comply with the Data Protection Act and to encourage them to adopt good practice. The code aims to strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate

interests of employers in deciding how best, within the law, to run their own businesses. It does not impose new legal obligations.

6. MANAGEMENT OF RISK

	Risk	Low (L), Medium (M), High (H)	Mitigation
Financial	Non-compliance with applicable Data Protection law may lead to enforcement action with monetary penalties and/or financial liability for damages to customers. If the Council does not have an adequate policy in place, there is a real risk that the Council will not be able to use the PSN.	L	Implementing protective monitoring and the adoption of this Protective Monitoring suite of documents will mitigate the risks by identifying potential breaches and demonstrating sound governance.
Legal	Any investigation may give rise to legal challenge. Having adequate policy and practice in place reduces the likelihood of a successful challenge	L	By agreeing the recommendations legal risks are minimised due to evidence of due diligence and consideration of the listed acts and regulations. The document 'Protective Monitoring Risk Assessment' further highlights the risks to the business in performing or not performing protective monitoring.
Employee	Without adequate Protective Monitoring, employees, elected members and others may have their personal data compromised by security breaches, and malware attacks and with a lack of nonrepudiation may be falsely accused of inappropriate actions	L	By agreeing the recommendations risks are minimised for the employee due to policy, procedure and supporting material being documented and communicated. The document 'Protective Monitoring Risk Assessment' further highlights the risks to the individual in performing or

	Employees, elected members and others may be concerned that senior officers are looking through their private correspondence.		not performing protective monitoring. Appropriate measure means that in regard to employee, elected member and other accounts that information is only accessed when absolutely necessary, to the level of detail absolutely necessary.
Customer	Without appropriate protective monitoring, customer data would not be secure breaching legislation. A data breach where protective monitoring was not in place would mean that a significant fine imposed on the Council by the Information Commissioners Office. If the Council does not have an adequate policy in place, there is a real risk that the Council will not be able to use the PSN thereby affecting our service to the public.	L	Implementing protective monitoring and the adoption of this Protective Monitoring suite of documents will mitigate the risk by identifying potential breaches and demonstrating sound governance.
Environment	None	L	
Technology	Without Protective Monitoring, a security breach would infect the Council's IT system.	L	Implementing protective monitoring and the adoption of this Protective Monitoring suite of documents will mitigate the risk by identifying potential breaches and demonstrating sound governance.
Reputational	Realisation of any of the above risks would also be likely to lead to significant reputational damage to the Council.	L	Implementing protective monitoring and the adoption of this Protective Monitoring suite of documents will mitigate the risk by identifying potential breaches and

	If the Council does not have an adequate policy in place, there is a real risk that the Council will not be able to use the PSN.		demonstrating sound governance.

7. OUTCOMES

Local Outcome Improvement Plan Themes	
	Impact of Report

Design Principles of Target Operating Model	
	Impact of Report
Governance	Formally documenting 'Protective Monitoring' ensures the essential governance is in place.
Workforce	'Protective Monitoring' emphasises a culture based around safety and security.
Process Design	'Protective Monitoring' underpins business processes and objectives where these are being conducted electronically.
Technology	'Protective Monitoring' is a key element in any technology we introduce which aims to keep the business, the workforce and the public safe.

8. IMPACT ASSESSMENTS

Assessment	Outcome
Equality & Human Rights Impact Assessment	Required
Privacy Impact Assessment	Required
Duty of Due Regard / Fairer Scotland Duty	Not applicable

9. BACKGROUND PAPERS

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

9.2 Standards

- ISO27001/2
- PSN

9.3 Regulations

- PCI DSS

9.4 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.

10. APPENDICES (if applicable)

Appdx 1 Protective Monitoring Policy
Appdx 2 Risk Assessment
Appdx 3 Access to Information Procedure
Appdx 4 Access to Information Guide and Form

11. REPORT AUTHOR CONTACT DETAILS

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