Protective Monitoring Privacy Impact Assessment

The need for a PIA

The impact assessment has been carried out to demonstrate that Aberdeen City Council is compliant with:

- The good practice recommendations contained in the UK Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work.
- The good practice recommendations contained in the UK governments National Cyber Security Centre (NCSC) Good Practice Guide 13 - *Protective Monitoring* (GPG 13).
- **The Human Rights Act 1998** which suggests that employees have a reasonable expectation of privacy in the workplace.
- **The Regulation of Investigatory Powers Act 2000** which covers the extent to which organisations can use covert surveillance.
- **The Data Protection Act 1998 (or subsequent iterations).**
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Other relevant legislation.

This impact assessment was prepared by the Council's IT & Transformation Team in conjunction with Legal Services and Human Resources and Customer Service.

The subject of this impact assessment is the continuous electronic monitoring of external communications to and from the Council's ICT network, and the recording, storage, reporting, and disposal of data relating to external e-mail and Internet usage.

Applicability

This impact assessment relates to User activity as a result of their use of ICT Resources provided by the Council.

Electronic and Human Threats

The following threats have the greatest potential to adversely affect the Council, its Users, infrastructure and electronic data:

a) **Electronic attacks.** These take the form of such things as denial-of-service attacks and the introduction of viruses, spyware and unsolicited e-mail. These have the following main effects:

- Overloading the ICT infrastructure.
- Corrupting components of the ICT infrastructure or replacing existing components with unauthorised ones, thereby causing ICT systems/services to become unreliable or unstable.
- The unintended introduction of malicious computer software

which has the ability to monitor Users access to/usage of ICT systems/services and (without Users' knowledge) send data to unknown recipients.
- Unsolicited e-mail (commonly referred to as 'spam', 'phishing' and 'spoofing') being sent to Users.
- Ransomware infection which prevents access to your data (sometimes permanently) and demands a ransom for it to be released.

b) **User access.** Access to and usage of the Council's ICT computer systems, services and electronic data. Such access/usage includes access to the Council's and externally provided systems/services. These have the following implications if not accessed/used appropriately:

- Access to dubious Internet sites resulting in the accidental downloading of viruses, spyware and unsolicited e-mail (which could have the effects outlined at a) above).
- The Council's ICT infrastructure and electronic data being corrupted, making computer systems/ services inaccessible – with electronic data becoming corrupted or inaccurate.
- The Council being unable to fulfil its statutory obligations.
- The Council's reputation being damaged and/or the Council being exposed to litigation.
- Disciplinary and/or criminal law action being taken against individual Users.

Whilst the majority of the threats described above are mitigated by the electronic security systems which the Council employs (e.g. through the automatic interception and deletion of viruses and spyware before they are able to cause damage or disruption), these systems can never be wholly effective and it is therefore important that the Council has an electronic monitoring capability which allows for:

a) The identification of malicious activity where it has not been automatically detected.

b) The electronic monitoring of Users' access to or usage of its computer systems, services and electronic data in order to provide assurance that the ICT AUP is being complied with and that the Council and its Users exposure to the stated threats is as low as practicably possible.

c) Trend analysis to take place to look for patterns of activity which may indicate a precursor to an attack or an attack in progress.

ICT Service Delivery

IT & Transformation has responsibility for managing the ICT infrastructure and are the custodians of data stored on the infrastructure. The ICT infrastructure makes this data available to Service Areas.

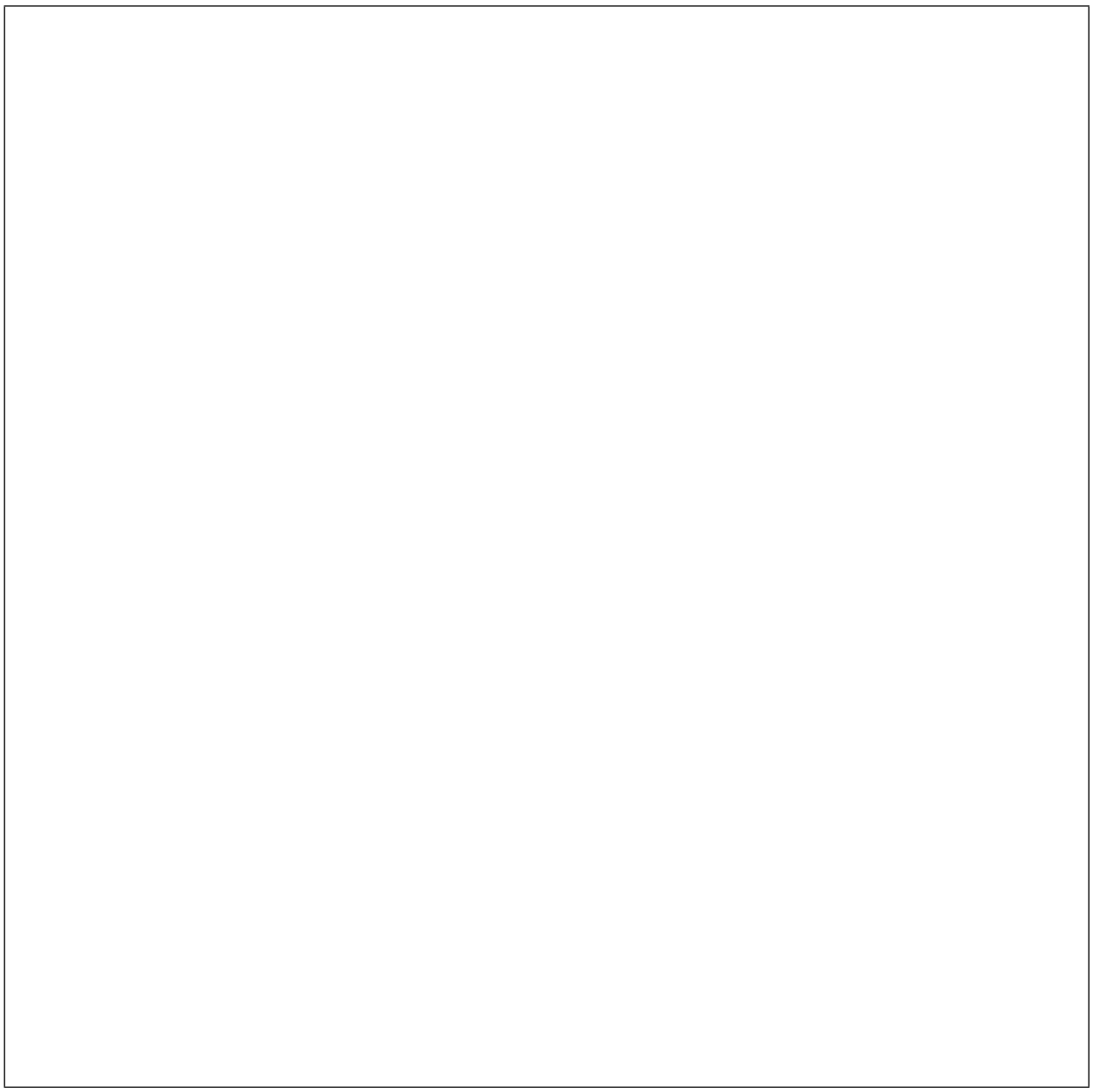
The Council is heavily reliant upon its ICT infrastructure to support its statutory obligations and to deliver front-line services. The Council is under constant scrutiny to demonstrate proper control over, and accountability for, the use of public funded resources. It is therefore desirable that the Council reduces the risk of loss or interruption to services by recognising threats affecting its ICT infrastructure and employing suitable countermeasures.

In order to identify vulnerabilities, threats and business risks the Council arranges an IT Health check (ITHC) annually which forms part of our submission for the Public Services Network (PSN) for compliance and a quarterly specific scan is run to ensure Payment Card Industry (PCI) compliance. A program of works is put in place to mitigate any significant vulnerabilities identified.

The Council reviews published information and research, is a member of the Cyber Security Information Sharing Partnership (CISP) and part of the well-respected (Scottish) Local Authorities Information Security Group (LAISG).

Countermeasures employed by the Council include a combination of written policies and technical countermeasures. Policies inform Users of the Council's expectations in the use of the ICT infrastructure, and the technical countermeasures support the policies, by enforcing good practice and reducing the potential for vulnerabilities to be exploited.

The ICT Acceptable Use Policy (Hyperlink when on the Zone) AUP is the Council's main ICT user policy. It is regularly updated to take account of developing threats and exploitation of vulnerabilities. Technical countermeasures are employed to detect the most prevalent malicious electronic threats associated with spyware, viruses and malware on computers and in Email attachments and to detect spam, phishing and spoofing activity, all of which have a real potential to degrade or interrupt the use of data in the ICT infrastructure.



The Information Flows

Technical Countermeasures

The technical countermeasures currently in use are ICT security systems specifically designed to operate in an integrated security environment.

Antivirus countermeasures are applied to incoming/outgoing e-mail to check for patterns that indicate the presence of malicious software in attachments.

E-mails are also checked for known spam, phishing and spoofing patterns. Where these are recognised, they are removed so that they do not adversely affect the ICT infrastructure. Known Spam e-mails are automatically deleted.

Antivirus and End Point protection on PCs and Laptops provide a further layer of protection against malicious software that manages to bypass security measures at the gateway or are introduced through another medium.

Countermeasures applied to Internet access can also remove malicious software from downloads; this is limited to known threat patterns. Internet access is further safeguarded by the ability of the ICT security software to block access to web-sites which have the potential to be non-compliant with the ICT AUP.

Other countermeasures include Intrusion Prevention Systems and Event Correlation.

These technical countermeasures cannot cover all eventualities however, and because of constantly growing and changing threats there remains the potential for undetectable malicious software entering the ICT infrastructure.

The ICT security systems record and maintain records of Internet and email usage and can therefore be used to help detect possible compromise and determine overall compliance with policy.

Purpose

The Council's main purpose in establishing its monitoring arrangement is to enable Corporate Governance to undertake lawful monitoring in order to support the Council's service delivery.

Continuous electronic monitoring of incoming and outgoing e-mail messages will be undertaken for the purposes of identifying activity and content which is likely to breach the ICT AUP.

Continuous electronic monitoring of the content of outgoing and incoming e-mail attachments will be undertaken for the purposes of detecting and removing where possible viruses/spyware, malicious software and content and for identifying activity and content which contravenes the ICT AUP.

Continuous electronic monitoring of Internet access will be undertaken for the purposes of detecting, removing or preventing where possible inadvertent access to instances of spyware, viruses, malware and other malicious software.

Continuous electronic monitoring of Internet access will be undertaken to block attempts to access web-sites which contain malicious content or that do (or are likely to) breach the ICT AUP.

Scope (of Monitoring)

Monitoring will apply to all Users' external e-mail and Internet facilities.

Continuous electronic monitoring of e-mail messages and attachments will apply to external e-mail only (i.e. those e-mails coming from or going to other networks, primarily via the Internet). This is mainly an automated process, but manual intervention is necessary for clarification/confirmation purposes and to manually delete blocked email or to release it where it does not contravene the ICT AUP

Transactions about Internet and e-mail activity will be recorded. Access will be provided to recorded transactions, where there is lawful reason to do so, in order to investigate allegations of improper use of the ICT infrastructure in line with the Access to Information Procedure (Hyperlink when on the Zone).

Records will be continuously and automatically retained by the respective monitoring systems and backed up to the corporate back-up facility at the end of each working day. Records will be held on the respective monitoring systems for 6 months, with data older than that being progressively deleted. Security measures are built in to protect the collected data which will only be accessible by authorised persons.

In the case of Emails, although the logging records are deleted the Emails themselves remain in users in-box, sent items and archives. Emails are also sent for backup every night.

Consultation requirements

Reporting and Accountability

Records will be used to produce statistical reports on request for senior management, and to provide detailed user-specific reports to support investigations.

The statistical reports are intended to provide senior management with a general analysis of email and Internet activity in order that informed decision can be made about the acceptable use of internet and external e-mail

Adverse Impact

In preparing this impact assessment, views of concerned parties have been researched, and the published articles by UNISON, ACAS, legal professionals, the Information Commissioner and others have been studied and evaluated in order to satisfy the Council's founding principle of 'openness and transparency'. The table below contains generally expressed concerns about monitoring (which concerns are catered for by the UK Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work) and the Council's rationale for undertaking continuous electronic monitoring. The intent is to allay such concerns by justifying the need for monitoring, thereby striking a balance between the rights of the organisation and the rights of the individual.

	Employee Concerns	Monitoring Rationale
1	Users may hold the view that monitoring is excessive as every activity is recorded.	Keeping good comprehensive records is essential to protect organisations and individuals from growing threats. For example, 'identity theft' can be verified by reference to the organisation's records of usage. This would not be possible if records were incomplete.
2	Users may be concerned that monitoring is intrusive and that information of a personal nature may be collected and disclosed without their knowledge, or as a result of an unrelated investigation.	All monitoring will be lawfully implemented and will be both controlled and accountable. Technology is used to automate, as much as possible, the monitoring process, to handle the huge volume of information, and to produce accurate results, which is in everyone's best interests.
3	Users may be worried that they may be blamed for actions which were not theirs, following well-publicised e-mail and Internet scams.	Monitoring can be used to stop threats e.g. spam; phishing; and spoofing, and to help identify who initiated them - interruptions to service delivery are minimised, and Users' experiences of worrying security incidents are reduced. Monitoring can also help to prove that no wrong-doing has taken place
4	There may be a concern that monitoring affects morale, is demeaning, and causes stress - the pressures upon Users to deliver service requirements are further increased by a perceived lack of freedom to use technological resources without undue scrutiny.	The Council has set practical limits to areas of monitoring - for example, internal e-mail is not monitored.
5	Monitoring arrangements may be seen as lack of trust – Users cannot be trusted to adhere to the rules.	Monitoring assists compliance checking to show good use of public funds - traceability ensures that Users are accountable for their actions, and encourages good-practice use of the technological resources. Raising management awareness enables timely preventive action to reduce noncompliance.

Alternatives (to Monitoring)

In producing this assessment, Corporate Governance recognises its management responsibilities regarding the infrastructure and as custodians of valuable data upon which the Council is heavily reliant. Corporate Governance takes these duties very seriously and employs resources which help to protect valuable assets from harm, but to be optimally effective the

responsibility for protecting these assets must be shared by the whole organisation i.e. by individual Users.

Whilst protecting valuable resources is a business process in its own right, it should also be seen as an intrinsic part of the day-to-day working and strategic business objectives facing the organisation. With this in mind, the proposed monitoring arrangements have been considered alongside the following alternatives:

a) **A policy-only approach**. Security policies define the expectations of an organisation's desire for good practice in the use of ICT resources. A policy-only approach delegates most of the security responsibilities to Corporate Governance, without it having all necessary means to monitor/measure overall compliance with policy.

b) **Good practice advice and guidance approach**. This approach is taking shape and several documents have been produced and launched using the Council's Intranet (the Zone). This approach is driven by Corporate Governance and, like the policy only approach, relies on feedback to verify effectiveness. Good practice advice and guidance is necessarily generalised and reactive, and is best used to reinforce and support policy

c) **Education and Training (E&T) approach**. Corporate Governance does not have the resources to provide extensive E&T. Effective E&T requires a clear service-level understanding of endemic or widespread vulnerabilities. Whereas Corporate Governance can provide advice and guidance, the nature of service-level vulnerabilities are best understood and provisioned by senior management. This impact assessment supports senior management involvement in understanding service-level vulnerabilities.

c) **Audits, spot checks, self-compliance verification.** Given the extremely high scale of Internet and e-mail activity in the ICT infrastructure, finding and testing a representative sample presents a considerable challenge as well as requiring detailed scrutiny of material in the sample in order to verify compliance. The nature of cyber threats makes sampling ineffective.

d) **Temporary or random monitoring.** This form of monitoring using technical countermeasures will only record data for the time when it is active. An incomplete set of records will not give the full picture; an incomplete set of records will be of no value to internal investigations or when handling allegations of improper use brought by persons or organisations outside of the Council. The nature of cyber threats makes random monitoring ineffective.

Privacy and Related Risks

See Protective Monitoring Risk Assessment (Hyperlink when on the Zone).

Privacy Solutions

In order to keep the privacy impact at a minimum while enabling a high level of security:

Automated tools are used which enable the blocking of identified spyware, viruses, malware, malicious software, Spam and phishing Emails

Automated tools are used which enable the blocking of access to websites which are known to be of high risk or are inappropriate whether due to compromise, viruses, malware, malicious software, containing controversial material.

Automated tools are used to identify and help protect against other threats such as intrusion attempts or denial of service attacks.

Access to any logged information relating to a user requires to be done by authorised personnel and using separate Administrator privilege accounts.

Access to any logged information relating to a user for investigatory purposes requires authorisation and completion of the Access to Information Form (Hyperlink when on the Zone).

Reports that are produced to identify possible compromise or due to a particular unusual event contain the minimum information necessary to analyse the situation. This information is restricted to those key staff performing the analysis, is stored securely and deleted if not required. In the event that analysis shows further investigation is warranted, authorisation and completion of the Access to Information Form (Hyperlink when on the Zone) is a requirement.

Sign off		
Risk	**Approved solution**	**Approved by**
Protective Monitoring	See Protective Monitoring Risk Assessment (Hyperlink when on the Zone).	Simon Haston (SIRO)

Integrating the PIA outcomes back into the project plan N/A		
Action to be taken	**Date for completion of actions**	**Responsibility for action**
Contact point for future privacy concerns		

Related Policy Document Suite

Policy and Strategy

- ICT Acceptable Use Policy
- Employee Code of Conduct

Procedures

- Access to Information Procedure (Hyperlink when on the Zone)

Forms

- Access to Information Request (Hyperlink when on the Zone)

Assessments

- Protective Monitoring Risk Assessment (Hyperlink when on the Zone)

Related Legislation and Supporting Documents

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).

Standards

- ISO27001/2
- PSN

Regulations

- PCI DSS

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.