SCOTTISH ENVIRONMENT PROTECTION AGENCY

Information Technology
Acceptable Use Procedure

SCOTTISH ENVIRONMENT PROTECTION AGENCY

Information Technology Acceptable Use Procedure

1. Procedure Statement

SEPA is required by the Scottish Government to comply with the requirements of the Cabinet Office Security Policy Framework and has to report annually on compliance. Effective performance and security of SEPA Information Technology (IT) resources relies upon its users adhering to established standards of proper conduct. The aim of this procedure is to ensure that all SEPA IT resources, that is systems, technology, networks, telephony, databases, data or other resources, are maintained in a safe and effective operational state so as to ensure the **C**onfidentiality, **I**ntegrity and **A**vailability (CIA) of the information held and managed by SEPA By doing so this assists SEPA to attain compliance with the Security Policy Framework.

This procedure defines the responsibilities of SEPA employees and all others offered use of SEPA IT resources. This requires efficient, secure, ethical and legal utilisation of SEPA IT resources and is in compliance with the mandatory requirements of the Cabinet Office Security Policy Framework.

Any breach of these provisions will be reported to the Departmental Security Officer (DSO), who has corporate day to day responsibility for all security matters. If a user is found to have breached or attempted to breach any of these provisions, disciplinary action may be taken, as a result of which, sanctions up to and including dismissal could result.

2. General Principles

2.1 This Information Technology Acceptable Use Procedure (ITAUP) applies to all SEPA staff and to anyone legitimately offered access to SEPA resources, for what ever purpose. No SEPA member of staff or other person shall be granted access to any SEPA system or equipment until they have successfully undergone the checks required by the Cabinet Office Baseline Personnel Security Standard. Any person granted access to SEPA IT resources, will hereafter be referred to as staff. Any person granted access to SEPA resources will have to confirm that they have read, understood and agreed to this document. The SEPA Logon Warning displayed on start up of each computer requires all uses to confirm this.

2.2 Use of SEPA IT resources is permitted and encouraged where such use is suitable and appropriate for business purposes and supports the goals and objectives of SEPA.

2.3 SEPA IT resources include, but are not limited to, internet and intranet facilities, email, telephone/fax equipment and such other electronic media and services that SEPA may make available to staff for business purposes from time to time, including the use thereof.

2.4 SEPA IT resources are to be used in conjunction with SEPA Security Procedures as laid out within Securing our Environment and within specific IT security procedures. In particular, staff must keep their passwords private at all times and shall not by any means provide them to any other SEPA employee or any other person. Please note that Information Systems (IS) staff do not require users' passwords for any purpose. Staff shall log off or lock any computer or electronic device they have been using on each and every occasion the device is left unattended.

2.5 All handheld mobile devices, including mobile phones, shall have passwords or pin codes applied to ensure that they only be used by staff for authorised purposes.

2.6 All information classified in terms of the Government Protective Marking Scheme shall be appropriately protectively marked to ensure that it is managed, accessed, stored, used and

handled correctly. . Protectively marked information should not be taken outside of SEPA offices unless this has been authorised by the Information Asset Owner (IAO), DSO or the Information Technology Security Officer (ITSO) If, under authorised conditions protectively marked information is being taken outside of a SEPA office on an electronic device, that information must be protected to the appropriate levels. The ITSO will provide definitive guidance on the levels of protection based upon guidance in Securing our Environment and related government guidance and standards. Advice and guidance on what measures shall be applied to secure the information should be sought from the Departmental Security Officer (DSO) or the Information Technology Security Officer (ITSO). A copy of Securing our Environment is available on QPulse.

2.7 SEPA IT resources are to be used in a manner that is consistent with SEPA's corporate values and as part of the normal execution of an employee's responsibilities.

2.8 SEPA supports the premise that SEPA IT resources may be provided for the use of staff in conjunction with Union business, as per the terms of the Recognition Agreement between SEPA and the Trade Union, where this does not compromise or conflict with SEPA business use. However, Union use does not include use for any business or company not connected with legitimate Union business use. Union use is acceptable where such use is conducted with a sense of responsibility, is in line with SEPA corporate values and is in accordance with this procedure. Such use is generally subject to SEPA Corporate Management approval and may be removed at the discretion of SEPA Corporate Management at any time. SEPA Senior Management team or Business Management Team may also remove or limit use, including personal use of SEPA Information Technology resources for individuals or groups of individuals at any time for business and management reasons. User conduct is subject to SEPA policies, procedures and guidance, as well as relevant legislation.

2.9 SEPA supports the premise that SEPA IT resources may be used for the personal use of staff where this does not negatively impact upon the efficient and effective use of the systems for business operations, or compromise or conflict with SEPA business use. However, personal use does not include use for any business or company not connected with legitimate SEPA business use. Limited personal, non-SEPA use is acceptable where such personal use is conducted with a sense of responsibility, is in line with SEPA corporate values and is in accordance with this procedure. Such use is generally subject to SEPA Corporate Management approval and may be removed at the discretion of SEPA Corporate Management at any time. SEPA line management may also remove or limit use, including personal use, for individuals or groups of individuals at any time in specific cases of misuse or for other business reasons. User conduct is subject to SEPA policies, procedures and guidance, as well as relevant legislation.

2.10 SEPA through the Departmental Security Officer also retains the right to (and may in certain circumstances be required to) report any inappropriate or illegal activities to the relevant authorities.

2.11 Inappropriate staff use of SEPA IT resources, whether for business or personal use, can result in any or all of the following negative impacts on the organisation:-

- Reduced employee activity;
- Increased demand on available IT/network resources thereby impacting upon the efficiency of the system and of SEPA business;
- Jeopardising of both business and personal security;
- Jeopardising SEPA information;
- Legal liability;
- Adverse publicity and damage to reputation, either SEPA or personal.

Staff should be aware that in addition to corporate liability, personal misuse of SEPA IT resources could result in personal liability, both in terms of civil and criminal law, for staff. This

procedure therefore seeks to protect both SEPA and staff from deliberate or unintentional misuse of SEPA IT resources.

2.12 All staff should be aware that levels and patterns of IT usage (and in certain cases the content thereof) may be subject to monitoring, for security and resource management purposes, from time to time by SEPA. Employees should also be aware that:

i) The use of SEPA IT resources is subject to the parameters outlined in SEPA's own policies and procedures including, but not limited to, Dignity at Work. Any investigations into the use or misuse of SEPA IT resources will be carried out in accordance with SEPA policies and procedures. Any issues that relate to security, whether physical, information or accessibility, or that could give rise to risk to information in SEPA, shall be reported to the DSO.

ii) Most SEPA telephone content is not electronically monitored, although certain SEPA hardware may temporarily store a copy of content of faxes sent or received. Telephone and fax numbers and patterns of usage may be revealed by bills, statements, etc. Calls to and from the SEPA Communication Centre (SCC) are recorded routinely. The use of the recorded information is restricted by procedures within the SCC to authorised managers who must give a specific and valid reason for access.

iii) Internet usage and content is electronically monitored and may be reported from time to time for performance and management purposes and to ensure that SEPA's obligations at law are maintained.

iv) Email usage and content may be electronically monitored from time to time. Emails marked 'personal' or 'Union' (to indicate non-business use or Union Business use) will only be subjected to further, non-automated investigation in exceptional cases. Such exceptions will be for specific investigatory needs and be determined on a case by case basis. Authorisation for further, non-automated investigation of any usage or content will be on authority from a Director or his/her nominated representative. Normally, the member of staff concerned will have been informed prior to the further investigation commencing. In exceptional circumstances, and pertaining only to the specific circumstances under investigation, the staff member may not be notified, but this will be authorised by a Director of his nominated representative, in consultation with the DSO and under specific direction of legal advice.

v) Non-automated, detailed examination and recording of content will only be carried out by SEPA where patterns of usage or content identified in the automated reports suggest further investigation may be required under disciplinary procedures, or where SEPA has been given other grounds to believe this may be required, for example a complaint from another member of staff. Any issues that relate to security, whether physical, information or accessibility, or that could give rise to risk to information in SEPA, shall be reported to the DSO.

vi) Most IT usage is directly traceable back to individual users. Monitoring will include the user account used, dates and times of usage.

vii) SEPA may be required to release emails or electronic files under the Data Protection Act (DPA), Freedom of Information (Scotland) Act (FoI), and Environmental Information Regulations (EIR), or at the request of The Police or the Crown Office. All information, regardless of designation, location or title, will be releasable under warrant or a formal written request from the police or Crown Office. Any staff email or document not identified by its title or its location in a specified folder as personal could be deemed to be releasable under any of FoI/DPA/EIR requests. To avoid this, personal emails and files should be labelled in the subject line with the word 'personal' at the start. Any personal emails or files sent or received should be placed in a folder clearly marked, typically, as 'Personal Documents', and kept separate from SEPA business documents. It is each staff member's responsibility to advise those who may send personal emails to mark their emails as 'personal'. If such a non-business email is not marked as 'personal' and is monitored, staff will be responsible to the sender for

any breach of their privacy by SEPA monitoring or by the need to release under required regulations.

viii) Any monitoring undertaken by SEPA will comply with the relevant legislation and guidance, in particular the Data Protection Act, Regulation of Investigatory Powers Act, Computer Misuse Act and Part 3 of the Employment Practices Data Protection Code.

ix) SEPA may collect sensitive personal information as a result of monitoring. By using SEPA IT resources staff consent to this monitoring of personal information, including the collection of any sensitive personal data that may be contained therein.

2.13 The use of SEPA IT resources is subject to the laws of copyright, defamation, discrimination, computer misuse and UK and Scottish law in general.

2.14 Staff shall not use any SEPA IT resource:

i) To access, download, communicate or create any offensive, defamatory, obscene, sexually threatening or intimidating, pornographic (including pedophilic), indecent, inappropriate or otherwise objectionable comments, images or materials. This shall include, but be not limited to, anything that does or may reasonably be determined to be discriminatory on the grounds of a person's racial or ethnic origin, gender, sexual orientation, marital status, disability, political beliefs or religious beliefs. This shall also include anything that seeks to promote the use of controlled drugs or which seeks to glorify or promote terrorist, extremism or radicalisation or which is otherwise contrary to law. However, this is except to the extent permitted by a Director in furtherance of SEPA business, particularly for forensic analysis purposes (but not so as to permit any breach of the law).

ii) To visit internet sites that contain material described in 2.14(i) above, except to the extent permitted by a Director in connection with SEPA business, particularly for forensic analysis purposes (but not so as to permit any breach of the law).

iii) To make or post indecent, inappropriate, obscene or defamatory remarks, proposals or materials (which shall include, but be not limited to all items as specified in i) above) on the internet or intranet. For example, this includes material that is designed or likely to cause upset, intimidation or harassment of another person.

iv) To send or request any material that is offensive, sexually threatening or intimidating, pornographic (including pedophilic), indecent, inappropriate, obscene, or defamatory or which is intended to upset, harass or intimidate another person.

v) To upload, download or otherwise transmit any SEPA business information without the authority of the Information Asset Owner, In the event that SEPA business information that is not part of SEPA's normal communications with customers, stakeholders, board etc is to be legitimately transferred, reference must be made to both the Information Asset Owner and the Head of Information to ensure that data licensing conditions and security requirements are not breached. In particular, the management of certain datasets are covered by the Manual of Protective Security and shall be handled accordingly.

vi) To corrupt, disrupt access or change any other user's data, files, records or systems, except where explicit authority to do so has been given by the Information Asset Owner of a legitimate SEPA business process to which the system or information relates.

vii) To access, download or otherwise connect with any instant messaging, peer-to-peer (person-to-person or computer-to-computer) file sharing, on-line net radio, video broadcasts or any similar facilities, except where explicitly authorised to do so for SEPA business purposes by a Director or nominated representative and the Head of IS shall be informed. This includes but is not limited to MSN, Windows Live Messenger, Yahoo Messenger, ICQ or those chat services provided by social networking sites such as BeBo, Facebook or MySpace. This also includes explicit prohibition of video delivery from sites such as YouTube. You may contact the IS Helpdesk if you need more information on this.

viii) To connect to RSS (Really Simple Syndication) feeds from websites out with SEPA systems.

ix) To represent personal opinions as those of SEPA in any publicly accessible electronic format.

x) To allow an '@sepa.org.uk' or an @sepa.pnn.gov.uk email address to be published as a contact address on the internet for any purpose, particularly where this may be for personal or non-SEPA business use, except where explicitly authorised to do so for SEPA business purposes by a Director or the nominated representative and the Head of IS shall be informed.

xi) To connect SEPA computer hardware directly to the internet without specific prior approval Head of IS and only after appropriate safeguards have been put in place by SEPA IS Department.

xii) To download any software or electronic files to a SEPA device that does not have adequate security protection measures, including virus protection, that have been installed by SEPA IS, or otherwise to jeopardise the security and integrity of SEPA IT resources. If in doubt, advice must be requested from SEPA IS Department who will consider this as part of the SEPA Change Request process.

xiii) To download, install or load any programme or application on any SEPA IT resource that has not been **explicitly** approved in **writing** by SEPA IS Department.

xiv) To commit an act of malicious damage to any IT resources, belonging to SEPA or others.

xv) To transmit material such that this infringes the copyright of another person or entity.

xvi) To attach and use any peripheral storage device, including CDs, memory sticks or other removable media, which have been confirmed as meeting the required security standards by the ITSO. Without IS having installed approved security protection measures, including virus protection. These measures will be determined by the Head of IS from time to time.

2.15 SEPA staff must comply with the following with regards to email use:

i) Do not download attachments from personal email via a web interface (for example Hotmail or GMail) to SEPA devices, except where explicitly authorised to do so for SEPA business purposes by a Director or nominated representative and the Head of IS shall be informed. You may contact the IS Helpdesk if you need more information on this.

ii) Staff shall not send junk mail or spam. Spam or junk being defined as indiscriminate, unsolicited promotional email.

iii) All SEPA emails sent externally must include an appropriate disclaimer. The following wording is considered appropriate and should not be altered without consulting the Head of the Communications Department or his or her representative.

> *The information contained in this email and any attachments may be confidential and is intended solely for the use of the intended recipients. Access, copying or re-use of the information in it by any other is not authorised. If you are not the intended recipient please notify us immediately by return email to postmaster@sepa.org.uk*
> *SEPA registered office: Erskine Court, Castle Business Park, Stirling, FK9 4TR. Under the Regulation of Investigatory Powers Act 2000, the email system at SEPA may be subject to monitoring from time to time.*

iv) Access to SEPA email or systems from out with SEPA offices is available either directly through VPN (Virtual Private Network – a connection initiated by SEPA software on our computers to protect the equipment) or through the CITRIX (SEPA@HOME) Portal. Access through VPN is only permitted from SEPA computers. Staff shall not use any non-SEPA devices to access SEPA email or systems, either internally by direct connection or externally via VPN. Access via the CITRIX Portal, which connects through the public internet, is available from any internet connected device or computer, including non-SEPA personal or home computers.

2.16 Staff are reminded that any types of behaviour referred to herein or in the SEPA IT Use Guidance are demonstrative only and are not intended to form a prescriptive and/or definitive list. If any doubts exist as to any intended use of SEPA IT resources, this should be referred to either the ITSO or Human Resources prior to use.

3. Responsibilities

The responsibility for the implementation of this procedure rests with all SEPA managers with the support of the Human Resources Department. Responsibility in terms of providing relevant management information to allow SEPA to manage its IT systems rests with the Head of IS. Responsibility in terms of provision of security advice and incident reporting rests with the Head of Resilience supported by the ITSO. Review of this procedure will be carried out on a 24 month basis, or if required following a reported breach, to ensure it continues to meet legislative, organisational and user needs.

4. Monitoring and Reporting

Monitoring of internet traffic is performed by 2 separate automated systems. Internet page content is monitored using BLOXX (or another appropriate system) which identifies specific internet page activities against user accounts. Reports of activity can only be provided by specific request of a Director or nominated representative. On providing these reports, ITSO will also provide guidance on the interpretation of these reports. This also provides the ability to block certain content categories or Internet sites. Packeteer (or another appropriate system) monitors overall traffic types and provides prioritisation tools to assist with the management of Internet bandwidth. Reports are of a technical nature and not normally used outside of IS.

5. Procedure

Infringement of any provision set out in this procedure will be reported to the Departmental Security Officer (Head of Resilience) and will be handled through SEPA's normal disciplinary and grievance procedures.

6. Exception Management and Recording

In cases where exceptions to this procedure are required to be authorised by a Director the authorisation process will be managed by IS Helpdesk. All requests will be submitted on pro forma to the IS Helpdesk and will be reviewed by The Head of IS and the ITSO, or their nominated representatives, with appropriate recommendations made prior to submission to the Director or his nominated representative for approval. A record of all exceptions will be held by the IS Department.

Where authorisation from the Head of IS is required, the authorisation process will be managed by the IS Helpdesk. All requests will be submitted on pro forma to the IS Helpdesk and will be reviewed by The Head of IS and the ITSO, or their nominated representatives, with appropriate recommendations made prior to approval.

7. Implementation

All staff will be advised when this procedure is revised or updated. A copy of this procedure will reside in QPulse and on the HR intranet page.