SCOTTISH

CHILDREN'S REPORTER

ADMINISTRATION

INFORMATION SECURITY HANDBOOK

Title	Information Security Handbook
Version	Version 4.0
Date of issue	24 September 2021 (Final Draft)
Classification	OFFICIAL
Review date and by whom	September 2022 - Bruce Knight
Prepared by	Bruce Knight - Digital Security & Governance Manager
Reviewed By	Donna Redfern – Digital Services Manager 28 July 2021
	Stephen Eodanable – Data Protection Officer 15 July 2021
Consultation	HR Sub Group – 5 August 2021
Equalities and Human Rights Impact Assessment (EHRIA)	Submitted 20 July 2021
Approved by	Alistair Hogg – 17 September 2021
Document history	V4.0 Replaces all previous versions.

Information Security Handbook Structure

This handbook incorporates all of SCRA's Information Security policies and procedures to provide a single reference point for all SCRA Staff and those working for SCRA. The handbook is classified at the OFFICIAL level and protected accordingly.

Individual policies and procedures that make up the handbook are reviewed at the same time as the handbook so that when the handbook is issued they are the current versions of these documents.

The policies and procedures for the systems storing and processing OFFICIAL–SENSITIVE data (e.g. CSAS and RAVHI) are not included in the handbook as these are protected at OFFICIAL–SENSITIVE documents. Any users of these systems are required to sign a declaration that they agree to comply with the relevant policies and procedures as a prerequisite for obtaining access.

Revision History

The revision history below is only for the Information Security Handbook. The revision histories of all the documents that make up the handbook is available on Connect.

Handbook Version Number	Date	Change	Author
V1.0 (Draft)	11/09/03	First draft	B Deakin
V2.0	5/11/03	Approved by CMG	B Deakin
V3.0	5/03/14	New Framework includes all information security policies.	B Knight
V3.1	8/09/14	General update together with a new:- • Data classification policy; • Data handling requirements; • Incident management flow chart.	B Knight
V3.2	06/08/15	General update together with a new • Board lead; • SCOTS account management process; • Advice on phishing emails.	B Knight
V3.3	24/11/16	General update which included:- • Recognising ransomware as a real threat; • A new access to SCOTS procedure; • Information sharing - electronic exchange • New arrangements for sensitive cases in the CMS System Security Policy; • Add a new section – Document Roadmap;	B Knight
V3.4	29/10/18	Updates to:- • include references to SCRA's Data Protection Policy to meet GDPR and DPA 2018 requirements;	B Knight

Handbook Version Number	Date	Change	Author
		• reflect current SCRA roles and personnel and to improve clarity; • ensure the IT Service Desk Mailbox is used for emailing the IT Team; • include a new Cyber Security Policy; • updated the incident response flowchart; • reflect current requirements for BPSS identity documents; • include the use of a BitLocker passcode; • reflect changes in CMS training arrangements and access to CMS; • accommodate SCRA's Off-boarding Policy and Incident Recovery Plan; • include the use of private management folders; • include the use of privacy screens; • include the use of probationary user accounts for CMS.	
V4.0	24/10/21	The introduction of CSAS, retirement of CMS and GSi, and the pandemic has caused major changes to the technologies SCRA currently use, their threat profile and SCRA's Information Security Policy has been updated to reflect this. Notably there have been changes to:- • the Password policy (use of 3 random words); • SCRA's Access to SCOTS Procedure; • incorporate new collaboration tools - MS Teams, OneDrive, Vscene, Objective Connect, Yammer etc. • ensure that the handbook is current to SCRA's needs.	B Knight

Contents

1 Information Security Policy Statement

Version 1.5 24 September 2021

1.1 Objective

The objective of this Information Security Policy is to safeguard the confidentiality, integrity and availability of the information that SCRA holds. The introduction of SCRA's Agile Working Policy endorses home working and the objective of the SCRA Information Security Policy now extends to ensuring that information risks associated with home working are minimal.

Information is one of our most valuable assets and it is essential that we have adequate controls to ensure that it is not lost or compromised and we protect the rights and privacy of the individuals to which it relates.

1.2 Scope

The policy applies to all the information that SCRA holds, this includes information on individuals (both cases of children referred to SCRA and members of staff) and corporate information.

The policy applies to all forms of information[1] – paper, electronic, other media and oral communications.

The policy applies to all SCRA employees, including temporary staff and third parties engaged on SCRA business. Failure to comply with defined policy and procedures could be considered a breach of SCRA's Staff Code of Conduct and could lead to disciplinary proceedings.

This policy replaces SCRA's previous Information Security Policy in its entirety.

1.3 Policy

The purpose of this policy is to protect the information SCRA holds from all threats, whether internal or external, deliberate or accidental. This policy correctly applied and adhered to will achieve a comprehensive and consistent approach throughout SCRA, ensure business continuity, and minimise the occurrence and impact of security incidents and breaches.

It is the policy of SCRA to ensure that:

- Information is protected against unauthorised access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Information is shared in accordance with SCRA's statutory responsibilities.
- Information will be available to authorised personnel as and when required.
- Regulatory and legislative requirements are met[2].
- Business Continuity Plans are produced, maintained and tested.
- Information security training is available to all staff.
- All breaches[3] must be reported to the Information Governance team via the breach mailbox (breaches@scra.gov.uk) as per the reporting procedure.
- The organisational learning arising from examination of these incidents is widely available.

---

[1] This includes case files; information within SCRA's systems (CSAS, RAVHI, iTrent, eFinancials) and Connect; emails; information in electronic folders, laptops, memory sticks; paper files; faxes; handwritten notes; voicemail; verbal exchanges of information; MS Teams, Objective Connect etc.

[2] Requirements include The Data Protection Act 2018, The Computer Misuse Act 1990, the Freedom of Information (Scotland) Act 2002, the Children's Hearings (Scotland) Act 2011, the Human Rights Act 1998, etc.

[3] This includes any event that might have compromised the confidentiality, integrity or availability of a system or its information.

1.4 Roles and Responsibilities

Senior Information Risk Owner (SIRO)

The SIRO has direct responsibility for maintaining the Information Security Policy, providing advice and guidance on its implementation and will:-

- ensure the policy is reviewed regularly;
- ensure all information security breaches and incidents are investigated;
- ensure a log of all data breaches is maintained and reported to the Executive Management Team and Board on a quarterly basis.

Information Asset Owner (IAO)

All IAOs are directly responsible for classifying their information assets according to their business value and that their value to the organisation is fully exploited. IAOs ensure:-

- their information assets are handled and managed appropriately;
- containment of security incidents / data breaches and reporting them to the SIRO;
- that a register of their information assets is maintained and the security risks are regularly assessed.

Managers

- All line managers are directly responsible for implementing the policy within their team/business area and for adherence to the policy by their staff and relevant third parties;
- Line Managers ensure that known or suspected security issues are properly addressed and reported.

Employees

- All employees are responsible for adhering to this policy and other SCRA policies and guidance on information security;
- Report any known or suspected security breaches to their managers and the SIRO;
- Protect the information within their area of responsibility.

1.5 Related Policies[4]

- SCOTS IT Code of Conduct – applies to all users of the SCOTS[5] system. Available on Saltire - the Scottish Government's intranet.
- SCRA Business Continuity Plan
- SCRA Data Protection Policy
- SCRA Information Asset Owner Handbook
- SCRA Records Management Policy
- SCRA Staff Code of Conduct
- SCRA Disciplinary Policy and Procedures
- SCRA Whistleblowing Policy
- Advice for Staff – dealing with Social Media
- SCRA Information Sharing Guidance

Contacts:

Bruce Knight, Digital Security and Governance Manager

Gillian Henderson, Information & Research Manager

[4] Other SCRA policies and guidance on information security are currently being reviewed and updated.

[5] SCOTS is the name of the IT Managed Service provided by Scottish Government that SCRA uses.

2 Information Security Roles

Version 1.6 24 September 2021

SCRA is committed to complying with the UK Government's Security Policy Framework (SPF) and, in accordance with the SPF[6], has defined clear lines or responsibility and accountability through effective leadership.

2.1 Mandatory SPF Roles

Accounting Officer (AO): Neil Hunter, Principal Reporter/Chief Executive.

The AO has overall responsibility for ensuring that information risks are assessed and mitigated to acceptable level, and for discussing these at Board level. The AO role is to ensure that information risks are handled in a similar manner to other major risks such as financial, legal and reputation risks. The AO ensures that information risk is covered explicitly in the statement of internal control.

*(**Martin Toye** is the SCRA Board lead for Information Governance.)*

Senior Information Risk Owner (SIRO): Alistair Hogg, Head of Practice & Policy.

The SIRO is appointed by the AO and is responsible for managing SCRA's organisational information risks, including maintaining an information risk register. The SIRO is responsible for appointing Information Asset Owners.

Information Asset Owner (IAO)

The 5 key responsibilities of the Information Asset Owner are to:

- Lead and foster a culture that values, protects and uses information for the public good;
- Know what information the asset holds, and what enters and leaves it and why;
- Know who has access and why, and ensure their use of the asset is monitored;
- Understand and manage risks to the asset, and provide assurance to the SIRO;
- Ensure the asset is fully used for the public good, including responding to access requests.

Table 1 shows the SCRA's information assets together with their appointed owners.

Information Asset	IAOs
Case Information (Operational risks - Central / East)	Paul Mulvanny
Case Information (Operational risks - North West)	Helen Etchells
Case Information (Practice & Policy)	Alistair Hogg
Financial	Ed Morrison
Human Resources and Payroll	Susan Deery
Information within Connect and the SCRA website	Maryanne McIntyre
IT Infrastructure	Douglas Cameron
Strategy & Organisational Development	Lisa Bennett

[6] SCRA is to comply with the HMG Security Policy Framework May 2018 (SPF).

Table 1: SCRA's Information Asset Owners

2.2 Other Specialist SPF Security Roles

Bruce Knight as Digital Security and Governance (DS&G) Manager is responsible for information security on a day-to-day basis. He performs two SPF specialist roles, these are:-

- IT Security Officer (ITSO);
- Communications Security Officer (COMSO).

Business Continuity Manager: Paul Mulvanny, Senior Operational Manager.

The Business Continuity Manager is responsible for defining SCRA's contingency plans.

2.3 Other SCRA Roles

The following SCRA roles also have an impact on Information security:-

- **Gillian Henderson** as Information & Research Manager is responsible for data protection, freedom of information and records management within SCRA.
- **Stephen Eodanable** as SCRA's Information Governance/Data Protection Officer ensures that SCRA complies with data protection law.
- **Ian Allen** as Head of Property is responsible for the physical security of SCRA's premises.
- **Helen Mora** and **Crawford Gardner** as SCRA's Procurement Officer is responsible for ensuring that all new or extended contracts are cyber risk assessed so appropriate controls are put in place before the contract or contract extension is approved.

3 Use of IT Facilities

Version 1.5 24 September 2021

3.1 Assets Policy

- **Ensure all computer equipment is asset tagged.**
- **SCOTS users must always log off or lock their computer when leaving it unattended.**
- **Obtain management approval prior to removing equipment from SCRA's premises.**
- **Any consultants, agency workers and SCRA staff that are leaving SCRA must return any IT assets personally issued to them before they leave.**
- **End of life and broken equipment is to be disposed of securely.**

SCOTS Computers

If you have a desktop computer or laptop, then make sure it has an asset label (Blue, with a number to call if found, a bar code and asset number). Hearing laptops are SCOTS devices and staff should check that these laptops are tagged as SCOTS assets. Any member of staff finding that they are using a computer for SCRA business purposes without a SCOTS asset label must report this to the SCRA IT Service Desk.

Personal Electronic Devices (PED)

A PED is defined as any portable device that has the ability to store, process or transmit information, e.g. laptop, BlackBerry, mobile phone, tablet, secure memory stick etc. All PEDs are IT assets with nominated owners and records of their issue are kept by the IT Team in their IT asset register. If you have a PED, then you are responsible for its safekeeping at all times and you can be held accountable for its loss, if lost through carelessness on your part.

Removal of SCRA Property

Any removal of SCRA equipment, information, data or software from SCRA premises must be authorised by management and whilst offsite, must be subject to the equivalent degree of security protection as it has when in SCRA's premises.

Return of personally issued assets

Line managers are responsible for ensuring that all IT assets (PEDs) issued to their staff (including temporary staff, consultants and agency workers under their control) are returned prior to them leaving SCRA, or going on long-term absence (e.g. maternity leave, secondment). Line Managers should contact the SCRA IT Service Desk to find out what IT assets have been issued to their staff prior to them leaving. Line managers must also agree with the IT Team which assets are to be returned and which are to be kept so they can be reissued to new staff.

Disposal of Equipment

Disposal of IT assets is exclusively done by the IT Team. Contact the SCRA IT Service Desk if you have IT equipment that you no longer need or is broken.

3.2 Password Policy

- **Use strong passwords that cannot be guessed.**
- **Passwords used for accessing SCOTS or SCRA systems must not be the same as passwords kept for personal use.**
- **Do not disclose your password or PIN to anyone else and do not allow it to be accessible to anyone else.**

A user's password must have a minimum of 9 characters,

Characters Allowed:-

Letters: A – Z, a - z

Numbers: 0 – 9

Special Characters: @ # $ % ^ & * - _ ! + = [ ] { } | \ : ', . ? / ` ~ " ( ) ; and a blank space

The password must:-

i. Not contain a sequential string of numbers e.g. 123456 or characters e.g. abcde
ii. Not contain a well-known keyboard entry, e.g. qwerty
iii. Not contain more than 2 repeating characters, e.g. zzz
iv. Not contain more than two pairs of repeating characters.
v. Not be the same as the User ID.
vi. Not be transmitted in the clear or plaintext outside the secure location.
vii. Not be displayed when entered.

To avoid using commonly used passwords[7] such as *Iloveyou2* and *sweetheart*, users are encouraged to use:-

1. 3 random words of 4 characters or more, use at least one capital letter and separate them with blank character, number or special character, e.g. horse7Clock&tidy, or
2. select a suitable passphrase adding a number, a capital letter and special character into the passphrase e.g. Likeabridge£4overtroubledwater ,

Additionally

- Passwords or personal identification numbers (PINs) must be changed when it is suspected that others may know them;
- Passwords or PINs must not be made known to anyone else;
- If, in exceptional circumstances, there is a need to write a password or PINs down, then it should be stored securely in locked furniture or the office safe;
- Never record any login username or password on playback keys on your computer;
- Passwords or PINs selected for business use must be different to those chosen for personal use[8].

3.3 File Storage Policy

- **The G:Drive and H:Drive are the electronic storage areas assigned for staff usage.**
- **OneDrive – can be used to store and manage SCRA's OFFICIAL-SENSITIVE for up to a year.**
- **The C:Drive of desktop computers[9] must not to be used for storing SCRA data.**
- **Sensitive data must not be left in the scanner folder.**
- **The common folder is not to be used for storing sensitive data.**

[7] Attackers have access to lists of commonly used passwords obtained from breached websites.

[8] This avoids SCRA's information becoming vulnerable when the security of any public system is compromised.

[9] Desktop computers do not have their hard disks encrypted.

All staff with a SCOTS User Account are provided access to both a G:Drive and H:Drive each with a specific storage purpose. Although staff may be given access to other drives to perform their role, staff using workstations must not store SCRA information on their C:Drive. Laptop users have their hard drives encrypted so can store files on their C:Drive to facilitate offline working.

All staff are also provided with OneDrive, a Microsoft cloud temporary storage service that lets you store and protect your files, and provides the ability to share them with other SCOTS users. OneDrive provides a 10 Giga Byte storage space where all files are retained for a year since they were last saved, after which the file is automatically deleted.

Staff wanting to store sensitive business data can use OneDrive, but users must be aware of the risks. They must ensure that any sharing of sensitive data on their OneDrive is on a 'needs to know basis' and that the file is not to be shared with anyone external to the SCOTS environment.

All files stored on OneDrive that are to be retained for longer than a year should be transferred to the G Drive, and sensitive files should be stored in a restricted access folder for added protection. Contact the DS&G Manager if there is no suitable restricted access folder is available on the G Drive.

Case information is to be stored in the Core System and Applications Solution (CSAS) in accordance with SCRA's Data Protection Policy.

3.3.1 G:Drive

The G:Drive (Global Drive) is an SCRA workspace on SCOTS where you are able share information with other colleagues in your locality or team. The G:Drive, also known as the Corporate Drive, contains a scanner folder and a common folder[10] which have specific purposes as detailed below.

Scanner Folder[11]

Purpose: Temporary storage area for capturing scanned information from paper documents enabling the information to be transferred into other suitable storage areas.

Restrictions: Personal information (e.g. case information, staff information, etc.) and business sensitive data must be transferred immediately to folders that have restricted access, such as team folders on the G:Drive or onto the user's H:Drive. Once the scanning process (including the transfer of data) is completed, no data should remain in the scanner folder.

Scanner folder data will be reviewed and purged from time to time. Sensitive data found (if any) will be reported to the relevant IAO and removed from the drive.

Common Folder

Purpose: Temporary storage area for sharing general documents of interest with other users within their locality or office as an alternative method to email. The common drive can occasionally be used for transferring large files or entire folders containing personal information and business sensitive data between two restricted areas (see restrictions below)

Restrictions: If used for transferring large files or folders between two restricted areas then this must be done within the hour and all files associated with the transfer must be deleted immediately after the transfer is completed. There must be no residual personal information

[10] Localities that have moved to a single locality G:Drive do not have a Common folder.

[11] This is the scanner folder set up for general use and not the scanner folders set-up with restricted access to serve a specific business purpose.

(e.g. *case information*, staff information, etc.) or ***business sensitive data*** left on the drive after the data transfer.

General files older than a month will be periodically deleted. Sensitive data found left on the drive (if any) will be reported to the relevant IAO and removed from the drive.

Shared Workspaces

When there is a business need to share sensitive information between users who belong to different teams, e.g. for a cross team project, then MS Teams/channels could be used. This is a new SCOTS offering suitable for this type of sharing. For more information on how to set this up, please contact the SCRA IT Service Desk. Similarly, Connect can also be used for setting up shared workspaces, specify your needs by emailing the SCRA Communication Mailbox.

Private Management Folders

Managers who want to create a private folder for managing their staff should contact the SCRA IT Service Desk. The IT Team will arrange for a suitably named folder to be set up allowing only the manager and HR access to access it.

3.3.2 H:Drive

The H:Drive (Home or Handy Drive) is your own private storage space suitable for temporary storage of your own personal files, any reference files needed to perform your role, and any work in progress that you are not ready to share with colleagues.

ITECS have set a 2-year file retention policy for all files stored on H:Drives, after which the file can be automatically deleted and ITECS will not be able to recover the file. Corporate information held on the H:Drives must be transferred to the G: drive to avoid them being automatically deleted.

3.4 Permitted Personal Use

- **Must not be excessive and in the users own time.**
- **Usage must be within the law and subject to specific conditions.**
- **Store personal emails in a separate personal folder[12]**
- **Content filters restrict usage and all usage is logged.**

This policy statement defines permitted personal use and supplements SCRA's Internet and Email Usage Policy and the SCOTS IT Code of Conduct.

Email and internet services are provided to SCOTS users so that they are able to carry out the duties necessary to their role efficiently. SCRA permit users limited personal use of IT facilities. Content filters restrict usage and Information and Technology Services Division (iTECS) maintain logs of all email and internet usage. If SCRA Management suspect an SCRA user of abusing their personal use privileges, then this would be investigated as misuse of IT facilities.

SCRA supports personal use of SCRA's IT facilities on the provision that this is done in the user's own time (outside of working hours) and is not excessive.

Personal usage must be within the law and comply with this policy statement:-

- Emails should be brief and preferably without any attachments;
- Users should discourage incoming emails;
- Users must not use official templates for personal documents;

[12] This makes it easier to distinguish between personal and business emails so they are excluded when processing an FOI request.

- Sending of emails that are abusive, offensive, libellous or a nuisance is not acceptable;
- Users can prepare simple documents or spreadsheets on personal matters;
- Users must not use IT facilities for private commercial activity or for financial gain;
- Users must not generate or distribute chain emails.

Access to the following sites is **not acceptable**

- sites offering pornographic or other offensive material (e.g. racist material);
- Using the Internet for political activity;
- Externally provided[13] Web based mail[14] (e.g. Hotmail, Gmail etc.).

Staff are reminded that accessing SCRA systems (e.g. CSAS) for personal reasons is strictly forbidden.

SCRA users with a UNISON role are able to use SCOTS IT facilities for trade union activities relevant to their role.

SCRA users studying for any form of qualification, with SCRA support, may use SCOTS to prepare study material. Study should be completed in their own time and requires the approval of the user's line manager.

Any member of staff who makes improper or excessive use of the IT facilities may be investigated under the SCRA Disciplinary Policy and Procedures. SCRA retains the right to withdraw SCRA users' personal use of IT facilities, either individually or collectively, at any time.

3.5 Misuse of IT Facilities

- **Do not try to gain access to systems you are not authorised to use.**
- **Do not connect non-SCRA equipment to the SCOTS network or SCRA equipment[15].**
- **Do not modify any data you are not specifically authorised to update.**
- **Do not generate messages in a way that makes them appear to come from someone else**
- **Do not log on to a personal account other than your own.**

All usage of SCRA IT equipment whether this is supplied by iTECS or not must be in compliance with SCRA policies and the SCOTS IT Code of Conduct. The IT Code of Conduct defines IT misuse and gives examples of misconduct and of serious disciplinary offences.

Disciplinary Process

Any employee who violates SCRA security policies and procedures may be investigated under the SCRA Disciplinary Policy and Procedures.

3.6 Protecting SCRA Information

- **Adopt 'clear desk' and 'clear screen' policies.**
- **'Privacy screens' should be used when additional protection to sensitive information is required.**
- **Do not permit unauthorised access/use of SCRA applications/data.**
- **Do not use your SCRA laptop for accessing sensitive data in public.**

---

[13] SCOTS provide an internal web based mail service, which can be used.

[14] Unless a valid business reason for accessing webmail has been established and approved by the SIRO.

[15] SCRA equipment includes SCOTS equipment provided for SCRA use (e.g. laptops, desktops, printers etc.)

- **Ensure secure disposal of information.**
- **All printing is to be locked.**
- **Do not disclose your BitLocker passcode.**

All employees are required to take sensible precautions to protect SCRA's information at all times. Failure to secure information properly could result in SCRA breaching legislation and having to face legal action. This includes adopting a 'clear desk' policy, locking your computer when leaving your desk (clearing the screen) and locking any personal or sensitive information away when not in use. Staff should obscure coded locks from view when entering access codes to storage areas.

Any staff who feels that the sensitive data that they regularly access could be at risk should use a privacy screen to provide the additional protection they require. This risk could be from working by a window in view of bystanders, next to an aisle often used by visitors or contractors etc.

Care should also be taken when transporting SCRA's information to ensure it is not displayed or left unattended.

It is not acceptable to use SCRA laptops for accessing sensitive information in public places. This is a totally insecure environment and this practice is explicitly prohibited. Care must be taken to avoid your password being disclosed to a shoulder surfer.

Secure Disposal

Care should be taken when disposing of SCRA's information, see Appendix C – Handling of Classified Data for details on:-

- Disposal and destruction of physical papers.
- Disposal of CDs, DVDs.
- Disposal of data stored on magnetic or on electronic devices.

Where confidential waste consoles are not available staff must be aware of local arrangements for disposing SCRA's information. If unsure, contact the SCRA IT Service Desk for advice.

Printouts

To safeguard SCRA's information all printouts to printers must be locked. Printouts are not to be left on the printer unattended.

BitLocker Passcode

Data on SCOTS laptops are protected by BitLocker, which encrypts the laptop's hard disk and on power up, a BitLocker passcode is required to unlock the encryption. Any member of staff who has changed their BitLocker passcode must do so in accordance with SCRA's Password Policy. Users who have forgot their BitLocker passcode are to follow the BitLocker recovery process.

3.7 Remote Access Policy

- **Do not share/disclose any authentication keys or passwords.**
- **Always log out when leaving your computer unattended.**
- **Always shutdown your laptop at night.**
- **Do not access SCRA's sensitive information through a hotspot**

Remote Access to the SCOTS environment

Staff using an SCOTS issued laptop can access the SCOTS environment remotely through their home broadband or Wi-Fi set up at either at an SCRA office or at an SCRA outreach hearing centre (OHC). Although it is possible to connect to SCOTS through public Wi-Fi hotspots (for example in hotels or coffee shops) staff must not access SCRA's sensitive information through a hotspot as they are not secure.

Staff working from home who are experiencing problems getting access to SCOTS through their broadband are able to set up a hotspot on their SCOTS mobile devices so they can continue working – see Business Continuity Advice for laptop users.

For security reasons, laptops used for accessing SCOTS remotely must be switched off at night. If the laptop was stolen during the night the criminal would not need to bypass the BitLocker[16] screen and would only need to hack the SCOTS logon. Also, some security updates only take effect once the laptop has been rebooted so the laptop is more vulnerable if it is not rebooted daily.

Additionally

- Do not disclose your remote access password (if you have one).
- Do not attempt to remotely access an account that has not been authorised for remote access.
- Always log out of your account when finished.
- Never leave a logged on PC unsupervised.
- Do not permit unauthorised access to SCRA's systems, files or equipment.
- Take all reasonable steps to secure equipment and software from theft and accidental damage.
- Suitable precautions must be taken to prevent an unauthorised person from seeing sensitive information displayed on your computer when working remotely, such as, using a 'privacy shield', working in a private room (if feasible), etc.

CSAS

CSAS is hosted by Microsoft in the cloud so it is accessible through the internet. CSAS is configured so that all SCRA users must access CSAS through SCOTS equipment using a SCOTS approved web browser, this includes staff working from home. SCRA Staff are unable to access their CSAS user accounts using other devices which are not on the SCOTS network.

3.8 Software Policy

- **Do not install any software onto your computer.**
- **Do not make illegal copies of software.**
- **Keep software disks and manuals locked away.**

Copying Software

Do not copy software from somebody else's desktop device. You will probably be guilty of an offence under the Copyright, Designs and Patents Act. All software must be installed by the Information and Technology Services Division (iTECS) or by the IT Team.

[16] BitLocker is the Windows encryption technology that protects your data from unauthorized access by encrypting your drive. By entering the correct password into the BitLocker screen unlocks the encrypted disk.

Regular audits take place to identify the software running on each desktop device. You will not necessarily be aware that audits will be taking place, as they will be done remotely across the network where possible.

Anyone found with software that they cannot prove they have a license for, may be subject to disciplinary action.

If you have any doubts as to the legality of any software please contact the SCRA IT Service Desk.

Always keep software disks and manuals secure under lock and key. They will not only be useful, but are also proof of purchase.

3.9 Cyber Security Policy

- **All staff are required to complete a mandatory cyber-security eLearning course and refresh their training every two years.**
- **All software used on SCOTS is to be validated by iTECS first.**
- **Never switch off a virus checker.**
- **Learn how to recognise phishing emails and delete them immediately.**
- **Learn how to scan suspicious files for viruses.**
- **Learn what spoofing and mandate fraud is, and if unsure about a request - seek advice.**
- **A Risk Profile Assessment (RPA) is to be carried out on new contracts which involve the processing of personal information.**

Cyber-Security Training

As SCRA staff need to understand their information security responsibilities, all staff are required to complete a mandatory cyber-security eLearning course and refresh their training every two years.

Protection from Malicious Software

All employees are required to take sensible precautions to prevent and detect the introduction of malicious software. Computer software is vulnerable to unauthorised modification and a range of malicious techniques have been developed to exploit this weakness, i.e. computer viruses, malware, network worms, Trojan horses etc.

To avoid such problems, do not load or download software onto your computer - no games, no free gifts. All software used on the SCOTS network must be validated by iTECS first.

Malware

The most common route for malicious code to be downloaded onto your computer is through careless use of email and reading of attachments.

The protection of all SCOTS supported equipment is performed by iTECS, in the background, and does not usually require user involvement. If you are concerned that your antivirus software is not functioning correctly or are suspicious of a possible virus or a cyber-attack, please contact the Cyber Security and Defence Mailbox (cc SCRA Security Mailbox).

Phishing Emails

Phishing scams are the most common email cons as they are designed to look like they need a response (e.g. requesting payment of an invoice). They impersonate legitimate companies by using company logos in their emails (and in their fake websites) trying to trick you into supplying personal information, such as passwords, or into clicking on a link in the email to release malicious software (malware) which will infect your computer.

Spoofing and Mandate Fraud

In recent cyber-attacks aimed at SCRA, criminals have spoofed[17] a member of staff's email account, in the hope that recipient thinks the email is from a friend or work colleague and is caught off guard. The criminal's aim is to get the recipient to start communicating with them in the hope that they carry out their request.

Spoofing is commonly used to commit mandate fraud[18]. Staff dealing with requests to change bank details, or to make a payment of an unrecognised invoice, should treat these requests with suspicion. They must seek advice from their line manager or the Digital Security and Governance Manager before accepting that the request is genuine.

Ransomware Attacks

Phishing emails can be used to initiate a ransomware attack. When the user clicks the link in the email it triggers software that encrypts all accessible shared drives on SCOTS. Once the encryption is completed, the attacker demands a ransom fee in exchange for the decryption key. **Ransomware attacks are a real threat to SCRA and the SCOTS environment.**

Guidance is published on Connect that provides tips on recognising phishing emails. Any suspicious emails received on SCOTS should be forwarded to the Cyber Security and Defence Mailbox (cc SCRA Security Mailbox) so appropriate action can be taken to stop the spread of a possible attack. If in any doubt, delete the email immediately. Never respond to the email or click on any of the links provided.

All employees must note and report immediately to the SCRA IT Service Desk any software that appears not to be functioning correctly. If you suspect that the malfunction may be the result of malicious software (e.g. a virus or ransomware) you should:-

- Note the symptoms and any messages appearing on the screen;
- Stop using the computer and disconnect it from the network;
- Do not attempt to remove the suspected software from the computer and do not test the suspected software on any other machine;
- Report the problem immediately to the SCRA Security Mailbox.

Supply Chain Risk Management

Scottish Government have developed a Cyber Security Procurement Support Tool (CSPST) to help public sector organisations understand the risks associated with their suppliers.

A Risk Profile Assessment (RPA) is to be carried out as part of the due diligence process when the goods or services being procured requires the processing of personal information. The tool produces a report based on the answers provided at the RPA stage. This report provides:-

- a Cyber Risk Profile for this contract;.
- a Supplier Assurance Questionnaire (SAQ) based on this contract's current Cyber Risk Profile.

Suppliers will be asked to complete the Supplier Assurance Questionnaire on line, although a pdf can be sent to them if they prefer. The DS&G Manager will assess the answers provided and if they are satisfactory then the Procurement Officer will be informed accordingly. The DS&G Manager may seek further clarification from the supplier on some of the answers given, and if they are still not satisfactory, a decision will be made on whether the supplier is asked for a Cyber Implementation Plan (CIP) as a condition for awarding the contract to them.

---

[17] Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, websites and IP addresses.

[18] Mandate fraud is where someone tricks you into changing details of a direct debit, standing order or bank transfer by pretending to be someone (or representing an organisation) you trust.

3.10 Identification and Building Access Policy

- **All SCRA staff, visitors and panel members must wear identification badges at all times whist on SCRA premises.**
- **All personnel are to record when they enter and leave SCRA's premises.**
- **Staff are responsible for the safekeeping of ID badges and access fobs issued to them.**
- **SCRA staff should challenge anyone not wearing an SCRA identification badge whilst on SCRA premises.**

All SCRA staff are issued with photograph identification (ID) badges. Staff must wear valid ID cards on SCRA premises at all times. Staff must record when they enter and leave SCRA's premises.

Staff issued with key fobs for building access must ensure that their key fobs and ID badges are not worn together on a single lanyard.

All staff are responsible for the safekeeping of ID badges and access fobs issued to them.

All staff are empowered and encouraged to challenge anyone not wearing an SCRA identification badge whilst on SCRA premises[19]. If they are not comfortable with approaching a stranger then they should alert their line manager instead.

Return of ID Badges or Access Fob

ID badges are to be returned when they are damaged or if the member of staff is leaving.

Access fobs are to be returned if they are faulty or if the member of staff issued the fob is leaving SCRA or is starting an external secondment.

Loss of ID or Access Fobs

Any member of staff losing either their ID badge and or access fob are to report this immediately to their line manager.

Visiting Staff/Visitors/Contractors to SCRA Premises

All staff are responsible for their visitors/contractors for the full duration of their visit.

All visiting staff/visitors/contractors are to be asked to sign the `Visitors book' and provided with a `Visitors' ID badge. The ID badge number must be logged in the `Visitors book' alongside the visitors/contractors name.

All visitors/contractors are required to return their ID badge and sign out of the `Visitors book' prior to leaving SCRA's premises.

3.11 Incident Management Procedure

- **All cyber security incidents are to be reported immediately.**
- **All breaches are to be reported using the Breach Reporting Form.**
- **All IT security incidents, which have an impact on the SCOTS infrastructure, must be reported to ITECS using iFix.**
- **All CSAS incidents must be reported to the SCRA CSAS Helpdesk.**
- **All incidents involving SCRA's secondary systems or websites must be reported to the SCRA IT Service Desk.**

---

[19] Those invited to attend a children's hearing are required to sign in at the SCRA Hearings Reception and are not required to wear an ID badge.

Incident: An unplanned interruption to an Information and Communications Technology (ICT) Service or reduction in the quality of an ICT service, or an event that compromises the security of SCRA's information.

IT security incidents include security breaches, cyber-attacks, theft, threats, suspected weaknesses or malfunctions. Do not try to prove suspected weaknesses because your action may be interpreted as misuse of the system. If in doubt contact the DS&G Manager for advice.

Reporting Incidents

The incident management flowchart (see Appendix A) defines SCRA's incident reporting arrangements for all incidents that compromise SCRA's security and/or need an ICT fix.

Anonymous reporting of security incidents is permitted and details of the incident should be sent to the DS&G Manager or SIRO. The SCRA Whistleblowing Policy provides protection to employees who fear intimidation or reprisals because of reporting their concerns over security.

If any IT security incident has an immediate impact on the SCOTS infrastructure these must be reported to SCOTS immediately so they can decide what action is to be taken. All incidents affecting SCOTS are to be reported to Cyber Security and Defence Mailbox (cc SCRA Security Mailbox). Contact the DS&G Manager if you want to discuss your security concerns first.

Information Security Breaches

Information security breaches involving personal data (including breaches of Non-Disclosure/Rule 16) are to be reported in accordance with SCRA's Breach Management and Reporting Procedures. See Appendix A for examples of common breaches.

Responding to IT Security Incidents

The appropriate IAO is responsible for:-

- Containment of the incident to minimise impact and recovery from the incident;
- Assessing the on-going risk;
- Establishing the root cause of the incident and implementing preventative actions to avoid reoccurrence.

The SIRO is responsible for:-

- media handling with respect to the incident;
- notifying external regulatory bodies as appropriate to the type or security incident being reported;
- recording of all IT security incidents;
- approving corrective and preventative actions;
- disseminating lessons learnt.

The cause of all IT security incidents will be investigated and this will include checking if the incident was caused by the misuse of IT facilities.

Cyber security incident: This is defined by the National Cyber Security Centre (NCSC) as:-

- a breach of a systems security policy in order to affect its integrity or availability;
- the unauthorised access or attempted access to a system.

Examples include:-

- computer viruses;
- denial of service attacks;
- hacking;
- making unauthorised changes to an IT system.
- malware;

- misuse of IT systems.
- ransomware;
- unauthorised access to an IT system;

Reporting a cyber-security incident

All cyber security incidents are to be reported immediately to the SCRA Security Mailbox so the IT Team can take appropriate action to protect SCRA's data and systems whilst escalating the incident to the cyber security hotline. If the cyber incident involves personal data then the incident must also be reported to the SCRA Breach Reporting Mailbox.

3.12 Social Media

- **Any postings on social media which identifies children in the Hearings System is considered a breach and must be reported immediately**
- **To save any unwanted online comments/approaches, staff should not mention they work for SCRA in their personal profiles.**

SCRA is committed to using social media to aid communication and facilitate engagement. However, this increase in online activity brings risks for children, young people and families, as well as for SCRA staff and the organisation as a whole, and our partners in the Children's Hearings System.

The protection of children, young people and their families involved in the Hearings System is a key priority for SCRA. A deliberate or accidental posting on a social networking site, which identifies a child within the Hearing System, could have damaging consequences for the child and all those involved in their placement. If you are aware of a posting on social media that could be a breach, please alert your LRM/Press and Communications Manager immediately.

On personal social media accounts, staff should not state that they work for SCRA. Even on professionally relevant sites like LinkedIn, staff should consider whether it is necessary to state that they work for SCRA.

See Connect for more guidance on social media.

3.13 Personal Security Policy

- **All SCRA employees including temporary and agency staff are required to join the PVG Scheme[20] as a condition of their employment.**
- **Consultants working for SCRA must be security cleared before they are given access to SCRA information.**
- **Security clearance of all staff and consultants is in accordance with HMG Baseline Personnel Security Standard.**

Security Clearance

All SCRA staff and/or agency staff are required to be security cleared to the HMG Baseline Personnel Security Standard (BPSS), this includes joining the PVG Scheme as a condition of their employment. Joining the PVG Scheme is arranged by SCRA Human Resources.

All consultants requiring a SCOTS account are to be BPSS security cleared this includes a basic disclosure check as a condition to work for SCRA. Consultants are responsible for obtaining their own disclosure certificates. SCRA only accepts basic disclosure certificates that are less

[20] Protection of Vulnerable Groups (PVG) Scheme.

than six months old. Consultants working directly with children or vulnerable adults must be either PVG or enhanced Disclosure checked prior to their appointment.

The Head of Human Resources will be responsible for making decisions on employing staff who are listed or may potentially be listed under the PVG Scheme or using a consultant who does not have a clear disclosure certificate.

To comply with BPSS, staff[21], agency workers and consultants must supply 3 original identity documents:-

1) A current Passport *or* Photographic Driving license AND
2) An *original* birth certificate *or* Official Tax Document with your name and current address (P45, P60) AND
3) A utility bill *or* bank statement showing your address and dated within the last six months (mobile phone bills are not accepted).

New staff and consultants who have not obtained full security clearance must be treated as visitors to SCRA and must **not** be given access to SCRA sensitive data.

3.14 Information Sharing - Electronic Exchange

- **An Information Sharing Agreement has been submitted to the SOLAR[22] Group for approval, which when agreed with the local authorities, will set out the following:-**
  - The purpose for sharing and what categories of information will be shared;
  - the lawful basis for sharing the information;
  - how the information will be shared;
  - retention and disposal;
  - the necessary security requirements.
- **Secure electronic communications ratified by a Memorandum of Understanding (MOU) or an Information Sharing Protocol (ISP) are in place with some of SCRA's key business partners[23]**
- **Alternative arrangements are in place so that SCRA can communicate securely with others where there is a business need to do so.**

Data Sharing

Copies of our current Information sharing Protocols with SCRA's business partners are published within the Information Governance Document Library of Connect.

Police Concern Reports are sent by Police Scotland using Egress and these are decrypted at the SCOTS gateway. Standard Prosecution Reports[24] (SPRs) are sent directly to the Core System and Applications Solution (CSAS).

The Criminal Justice Secure Mail (CJSM) Service is used for secure communications between SCRA and safeguarders or defence agents. A list of current safeguarders is maintained on Connect and details of defence agents on CJSM are available on the External Contacts part of Connect.

---

[21] SCOTS use BPSS/10/08 V7 Form issued April 2017.

[22] Society of Local Authority Lawyers & Administrators in Scotland (SOLAR) is a professional public sector organisation whose aim and purpose is to support the work of those professional officers employed in local authorities and associated organisations in Scotland.

[23] Children Hearings Scotland (CHS) are the exception to this rule due to our joint responsibility to provide a service to the public.

[24] Sometimes called SPR2 as all SPRs send are Standard Prosecution Reports Version 2.

Cloud Services

iTECS has recently replaced Skype for Business with a new set of collaboration tools from the Microsoft 365 suite of applications. These are:-

- MS Teams, including chat, calls, meetings and teams & channels
- OneDrive
- Yammer
- MS Apps, including Forms, Delve, Planner and To Do

The data retention policies and intended usage differ for each of these applications, and staff must familiarise themselves with the guidance available before using these services.

Objective Connect is a SCRA provided service that provides secure external file sharing enabling our staff to have complete control over the information they share outside the SCOTS environment.

Vscene is a SCRA provided service providing staff with access to videoconferencing. SCRA staff now use MS Teams of the Remote Attendance Virtual Hearing Interface (RAVHI) for holding virtual hearings, so Vscene is now the backup solution when RAVHI is not available.

Contact the SCRA IT Service Desk for further information on these new services.

File Transfer Protocol (FTP)

A secure FTP solution is available to authorised staff who require to share bulk files securely with our contractors.

Approval from the SIRO must be obtained before using/accessing File Transfer Protocol (FTP) and/or document sharing sites like Google Drive, Dropbox or Amazon Cloud Drive.

4 SCRA Access to SCOTS Procedure

Version 1.6 24 September 2021

4.1 Purpose

This procedure defines the line management role in managing user access to the SCOTS service. It describes the process used by line managers to create new SCOTS accounts and to make changes to existing SCOTS accounts.

4.2 Scope

This procedure only deals with the creation of SCOTS user accounts and managing the users' access according to SCRA's business needs. The procedure does not cover when an employee is leaving SCRA as this is handled according to the SCRA Off Boarding Policy.

4.3 Responsibilities

Line Managers are responsible for:-

- ensuring that SCOTS Account Users who they line manage, have access to the resources they require to carry out the duties associated with their role;
- suspending users access when it is anticipated that the member of staff's (or temporary worker's) absence from work exceeds 4 weeks by becoming a long term absence and re-enabling their access on their return to work;
- ensuring that agency workers and consultants sign up to SCRA's Information Security Handbook using the third party agreement form (see Appendix B).

SCRA SCOTS Account Users are responsible for ensuring that their entry in the SCOTS Staff Directory is accurate and kept up to date. ***This is an essential requirement as inaccurate entries in the SCOTS Staff Directory will have a direct impact on logical access.***

The Digital Security and Governance Manager is responsible for:-

- keeping records that agency workers and consultants have signed up to SCRA's information security policies;
- recording any approved exceptions to this procedure and any agreed actions.

4.4 Definitions

Clone (Reference) Account: This is another user's account that is used by the system administrator to replicate the access privileges of that account over to a new or an existing account.

G:Drive: The G:Drive is a shared file storage area which allows SCRA users to share information with one another. The area is split into top level folders with different access rights for each folder enabling segregation of information on a 'need to know' basis.

Line Manager: The manager who SCRA staff (or temporary worker) reports directly to.

Long-term absence: Any continual staff absence from work that is greater than 4 weeks. For example if 3 weeks annual leave is taken and the staff member is then absent on sick leave with a medical certificate the absence then extends beyond 4 weeks to become a long term absence.

N Account/U Account: The account number is preceded by the letter 'N' or 'U' to indicate that the user is a permanent member of SCRA staff or has a contract that is longer than a year's duration.

Personal Information Updater (PIU) Form: By using the Staff Directory link on the home page of Connect, and the 'Click here to change your details' link provides the SCRA user with access to the Personal Information Updater (PIU) form. This enables the user to update their personal

details with respect to their role directly into the SCOTS Staff Directory. This information is utilised by SCOTS to provide access to resources within SCRA's public folders.

SCOTS Service: This is the name of Scottish Government network and the information services provided by the Information and Technology Services Division (iTECS) of the Scottish Government. SCOTS provided services include email, internet, shared file storage areas, public folders, Virtual Private Network (VPN) access, MS Teams, OneDrive, Objective Connect etc. through a SCOTS user login as well as telephony, video conferencing and OnSCOTS Wi-Fi.

SCRA SCOTS Account User: Either a member of SCRA staff or a temporary worker.

Temporary Workers: Consultants, Agency staff and any third party working on behalf of SCRA. This includes SCRA employees on short term contracts.

Z Account: The account number is preceded by the letter 'Z' to indicate the user is a temporary worker and the account has an expiry date.

4.5 Procedure

4.5.1 Information Security Responsibilities

Line managers must ensure that their temporary[25] workers sign up to SCRA's Information Security Handbook. Signed 'SCRA Information Security Handbook - Third Party Agreement' forms (see Appendix B) are to be sent to the Digital Security and Governance Manager.

4.5.2 SCOTS User Accounts

The line manager is responsible for managing their staff's SCOTS user accounts in good time to ensure no loss of service while at the same time safeguarding SCRA's systems and data.

Requests for new SCOTS accounts, or changes to existing accounts, are processed by the SCRA IT Service Desk to ensure quick and straightforward handling of on-boarding and maintenance of records using email templates available in the SCRA Manager's Checklist on Connect. There is an Outlook template that is to be completed for each category of SCOTS Account change.

These are:-

- New Account - to request a new SCOTS user account;
- Modify Account - to request a change to an existing SCOTS user account;
- Delete Account - to request for an existing SCOTS user account to be deleted;
- Suspend Account - to request suspension of a SCOTS user account;
- Re-enable Account - to request a SCOTS user account to be re-enabled as the member of staff is returning to work.
- Change of SCOTS User ID - when an existing staff member changes to a permanent or to a fixed term post;

The following change types are submitted by the line manager directly to iFix:-

- Change of Name/Email Address of an existing SCOTS user account;
- Extension to a Temporary Account – to make a request to extend the 'Expiry Date';

At least 5 working days' notice is needed for any changes to user accounts.

4.5.3 New SCOTS User Accounts

This email template is used to request a new SCOTS user account for Permanent and Temporary staff.

The line manager identifies a reference SCOTS user account (clone account) from which the access privileges can be copied. The new starter is provided G:Drive access and membership of the same groups as the reference account selected.

For temporary workers the 'Expiry Date' field must also be completed

[25] Excluding SCRA employees on short term contracts.

4.5.4 Modify/Change of Post

This email template can be used for 2 types of changes:-

Change of post: This change is required when a user is taking on a new role or changing their normal place of work. The line manager identifies a reference SCOTS user account from which the access privileges can be copied.

Additional Rights: When a SCOTS user is to retain their existing data access but to have additional requirements.

The user's line manager must initiate all changes above, by following the instructions within the iFix Service Catalogue for modifying accounts.

4.5.5 Delete

This email template must be used to delete a user's account.

The line manager should only also this form when a member of their staff's current absence from work is going to extend beyond 12 months as leavers are handled according to SCRA's Off Boarding Policy.

4.5.6 Change of SCOTS User ID

This iFix form is to be used when a member of staff moves from a temporary contract to a permanent contract or from a permanent contract to a fixed term contract. This change ensures that the letter (N, U or Z) in the User ID represents the correct employee status.

4.5.7 Extension to a Temporary SCOTS Account

The end user is notified of an account expiry in the weeks leading up to their end date. They are instructed within that notification to alert their line manager if the account is to be extended. Only the appropriate line manager, Locality Reporter Manager (LRM) or Locality Support Manager (LSM) have the authority to extend the 'Expiry Date' of a temporary SCOTS account. The extension is requested by completing the appropriate iFix form.

4.5.8 Suspend/Re-enable

SCOTS accounts can be suspended for a period of up to one year. A reason for this might be for a secondment, maternity leave, career break, long-term sick etc. If the period is longer than one year a SCOTS Access Delete request form should be completed.

A request is required by the appropriate line manager to re-enable the suspended account so it is ready for the member of staff returning to work.

4.5.9 Public folder Access

A change in a user's role whether temporary or permanent requires the user to update their personal information in the staff directory using the Personal Information Updater (PIU) form. Approval of the change will alter the user's access privileges for the public folders.

Where the access is required in addition to a user's current access, Modify/Change of Post request can be submitted detailing the additional access requirements.

4.5.10 Monitoring

The IT Team receive monthly reports from HR to monitor that all SCOTS User accounts are valid and are in line with current business requirements.

5 Email and Internet Usage Policy

Version 1.5 24 September 2021

5.1 Purpose

This policy defines acceptable usage of SCOTS email, and internet services and is applicable to all SCRA staff and anyone issued with an SCRA SCOTS account.

Failure by SCRA staff to comply with this policy may result in disciplinary action being taken in accordance with the SCRA Disciplinary Policy and Procedures, which could include action up to and including dismissal.

The Email and Internet Usage Policy does not define acceptable usage of social media. Instead this is defined in the Advice for staff – dealing with social media on Connect which applies to all SCRA staff whether they are accessing social media through SCOTS internet services or not.

5.2 Key Principles

Internet and email usage is to be within the law and to comply with the terms of this policy.

SCRA's email and internet services are provided by Information and Technology Services Division (iTECS) for work purposes.

Sensitive data exchanges must be appropriately protected and protectively marked.

This policy is based on the SCOTS IT Code of Conduct to which all users of the SCOTS Service agree to during log in, but imposes additional measures for valid business reasons.

SCRA defines specific usage requirements within this policy and expected standards of behaviour within the SCRA Staff Code of Conduct.

The processing of personal data must be in accordance with data protection laws and staff must comply with the SCRA's Data Protection Policy, and the policies within this handbook.

Email and internet usage is constantly logged by SCOTS, and SCRA will request access to SCOTS usage records if misuse is suspected.

5.3 Responsibilities

SCRA Users are responsible for familiarising themselves with the requirements of the SCOTS IT Code of Conduct and this policy and complying with them both.

The Digital Security and Governance (DS&G) Manager is responsible for recording any approved exceptions to complying with this procedure and why an approval was given.

Managers are responsible for ensuring that their staff are aware of and understand both this policy and the SCOTS IT Code of Conduct.

5.4 Personal Usage

Personal usage is permitted in the user's own time (outside of working hours). If the member of staff is on flexi, out of core working hour's usage is permitted provided this is not recorded on their timesheet as working. Usage is subject to the following additional conditions to those within the SCOTS IT Code of Conduct:-

- access to chat rooms and webmail[26] is prohibited;
- selling on the internet is prohibited.

[26] Unless a valid business reason for accessing webmail or a chat room has been established and approved by the SIRO.

Staff can use the internet for personal and family matters (e.g. banking, shopping etc.) and can communicate with others through social media provided the websites used are accessible through SCOTS. See Permitted Personal Use in the handbook for more detail.

5.5 Email Usage

Email filters are employed on the SCOTS email gateways to ensure that email content complies with the SCOTS IT Code of Conduct. When an incoming email is blocked, the intended recipient is notified by email. If it is presumed that the email is needed for business reasons then the notification email must be forwarded on to the Cyber Security and Defence Mailbox providing reasons why the email may be required so the email can be unblocked.

Staff must exercise caution when checking their emails in case they have been sent a phishing email. Using the guidance check that you recognise the sender and question why you have been sent the email. If in any doubt delete the email immediately. Any suspicious emails received on SCOTS should be forwarded to the Cyber Security and Defence Mailbox (cc SCRA Security Mailbox) so appropriate action can be taken to stop the spread of a possible attack.

Staff receiving emails which they consider to contain pornographic or offensive material, should close the document and advise their line manager and the Digital Security and Governance Manager.

5.5.1 Sensitive Emails

Emails that contain sensitive information must be protectively marked in accordance with the Protective Marking Emails guidance issued on Connect.

Before sending a sensitive email out staff should check that they are sending to a secure email address, these are published on Connect

An email containing sensitive or personal data must not to be sent to a non-secure email address. To prevent this from occurring users are not to set up auto-forwarding on their SCOTS email account to a non-secure email address.

5.6 Internet Usage

SCOTS employ internet filters to ensure that internet access complies with the SCOTS IT Code of Conduct. Occasionally staff need to access blocked sites for valid business reasons. If this is the case then the Digital Security and Governance Manager should be contacted.

6 SCRA Memory Sticks Policy

Version 1.3 24 September 2021

6.1 Purpose

The purpose of this policy is to safeguard SCRA's information by ensuring that only approved and registered secure memory sticks are used by SCRA staff and by defining acceptable memory sticks usage.

This policy applies to all SCRA staff and contractors.

6.2 Key Principles

Only approved types of encrypted USB (Universal Serial Bus) sticks[27] are permitted as the portable storage devices to which SCRA's information may be copied. Copying to portable media such as DVDs or CDs is only allowed in exceptional circumstances.

The use of **unencrypted** USB sticks is banned.

Only **approved** and **registered** encrypted USB sticks are to be used.

Ownership of memory sticks is monitored through the USB stick register and access to the memory stick is controlled through local records.

Encrypted USB sticks are to facilitate the transfer of personal or sensitive data to and from secure environments.

Encrypted USB sticks can also be used for non-sensitive information such as presentations.

Encrypted USB sticks are not to be used for long-term storage of SCRA information.

6.3 Exceptions

Occasionally there may be a business need to copy SCRA information to DVDs or CDs (e.g. for court), or use a secure memory stick to copy SCRA information to other environments (e.g. to give presentations externally, or to provide data to an external consultant or auditor). Where this involves personal or sensitive data, prior approval must be sought from the relevant Information Asset Owner.

6.4 Responsibilities

The responsibilities listed below are those relevant to this policy only. Breaches of this policy may be subject to consideration under the SCRA Disciplinary Policy and Procedures.

Encrypted USB Stick Users are responsible for:-

- safe usage under data protection laws and other relevant policies, such as SCRA's Data Protection Policy;
- the safekeeping of their encrypted USB stick(s);
- password management;
- returning their encrypted USB stick when it is no longer needed / leaving SCRA;
- ensuring a digital media declaration form is completed by the external party (e.g. court, defence agents), before handing over the secure memory stick, and for the safe keeping of this record;
- informing their line manager (or nominated memory stick owner) when their secure memory stick has been sent out to an external party, and who the external party is;
- retrieving the memory stick from the external party once they no longer need it;

[27] USB sticks are also referred to as memory sticks or pen drives.

- reporting the loss of a security memory stick immediately to the SCRA Security Mailbox;
- ensuring usage complies with this policy.

Managers (including LRMs and LSMs and Head Office Managers) are responsible for:-

- nominating a member of staff to be the registered secure memory stick owner for the pool of secure memory sticks purchased for the locality or Head Office team, and informing the IT Team by emailing the SCRA Security Mailbox;
- ensuring that only approved encrypted USB sticks are purchased;

Secure Memory stick Owners are responsible for:-

- informing the IT Team by emailing the SCRA IT Service Desk the numbers of USB sticks purchased so asset labels can be sent to them;
- adhering asset labels to the secure memory sticks purchased;
- keeping local records of who the security memory sticks have been issued to;
- ensuring that secure memory stick owners return their USB stick(s) to them when they leave;

Information Asset Owners (IAOs) are responsible for safeguarding information in their areas of responsibility. They must assess the business need of providing their information to others against the risks involved, defining what specific data handling controls are required to minimise the risk before granting an exception. Once an exception has been authorised the IAO must inform the DS&G Manager of the reasons behind the decision taken and what controls are in place to protect the information from unauthorised disclosure.

The Digital Security and Governance (DS&G) Manager is responsible for:-

- ensuring that SCRA has and maintains a USB stick register;
- recording any approved exceptions to this procedure and updating the information risk register accordingly;
- providing advice and guidance on data handling to the IAO.

6.5 Policy

Secure memory sticks should only be considered when there is no suitable means[28] of securely transferring SCRA's data out from the SCOTS environment to the those who have a valid business reason to receive it. Secure memory sticks provide temporary storage of the data to facilitate secure data transfer to another secure environment.

Only a few types of secure memory sticks have been approved by SCRA for use, and staff should contact their line manager in the first instance when there is a need for a secure memory stick. Localities must purchase secure memory sticks from their own budgets, and ensure that an asset label is adhered to all new secure memory sticks that they purchase.

Ownership of memory sticks is monitored through the USB stick register and access to the memory stick is controlled through local records.

Purchasing a new secure memory stick

Managers are to contact the SCRA Security Mailbox before ordering new secure memory sticks. The IT Team will be able to advise them on:-

- what the approved secure memory stick types are, and
- what suppliers may have these types of memory stick in stock.

[28] Email security may be in doubt, the size of the data set required is considered too large or complex for emailing out or uploading to a secure portal such as Objective Connect.

Asset Tags for New Secure Memory Sticks

Managers must inform the SCRA IT Service Desk of any purchases made so that an SCRA asset tag can be sent out to them for adhering to each secure USB stick purchased[29].

Registering New Secure Memory Sticks

Managers must inform the SCRA Security Mailbox of the asset numbers of their USB sticks and who the responsible owner is, so that the IT Team can register the memory sticks.

Local Records and Storage

The nominated memory stick owner must keep local records of whom the USB stick has been issued to and which memory sticks are available for use. Managers are to store their locality's pool of secure memory sticks in a locked cupboard. When a secure memory stick is issued locally, the record must be updated with the group of staff (e.g. receptionists) or the individual who will be responsible for the safekeeping of the memory stick from then onwards.

Secure Environments

Encrypted USB sticks are to facilitate the transfer of personal or sensitive data to and from secure environments. Recognised secure environments are corporate computers on networks connected to SWAN[30] and/or the PSN[31] i.e. the SCOTS network, the NHS network, Scottish Local Authorities networks, Police Scotland networks, Scottish Courts networks and SCRA standalone laptops. (A home computer is not considered to be a secure computing environment).

The member of staff responsible for the secure memory stick must ensure the external party completes a digital media declaration form before the USB stick is handed over to them.

Other Environments

Encrypted USB sticks can also be used to transfer non-sensitive information, such as presentations, to other environments.

Returned Secure Memory Sticks

Where the secure memory stick has been returned by a third party, the memory stick **must** be checked for viruses[32] and all the data wiped from the memory stick before the local records are updated to show that the memory stick is now available.

Individual Ownership

If an individual member of staff wants to take ownership of a secure memory stick, they must contact their line manager. The nominated memory stick owner must email the SCRA Security Mailbox providing the asset number of the secure memory stick given to the member of staff, and name of the individual so the USB stick register can be updated.

Old Secure Memory Sticks

There are a number of old secure memory sticks still in circulation that were issued to staff members several years ago. Many of them have been lost due to staff turnover, or used for sharing with external partners and were never returned. If a member of staff finds an old secure memory stick, they are to contact the SCRA Security Mailbox providing details of the memory stick found and whether they intend to take ownership of it, or not. These old memory sticks are identified by their serial numbers and/or by a permanent marker pen used to issue it a number e.g. MS 56.

---

[29] Asset labels are now used to identify new secure memory sticks as we found some manufacturers no longer print the serial number on the stick.

[30] Scottish Wide Area Network (SWAN)

[31] Public Services Network (PSN)

[32] The environment from which the memory stick was being used may have been infected by a virus or malware and the memory stick may have become infected too.

7 Mobile Device Acceptable Usage Policy

Version 2.3 24 September 2021

7.1 Purpose

The purpose of this policy is to ensure that all employees (including SCRA contractors) using SCRA issued mobile devices are aware of their security responsibilities.

7.2 Key Principles

Mobile devices are inherently vulnerable to loss and theft and therefore users must be vigilant when taking mobile devices out with secure environments, such as the office or home.

Kensington Locks **must** be used to secure laptops to immovable items to discourage theft.

Users must not access any personal or OFFICIAL–SENSITIVE information in public.

Remote access to CSAS must be through a SCOTS laptop using a VPN to connect to the SCOTS network.

Users should transfer the minimum data to the mobile device required for them to benefit from using the device.

Authentication credentials for mobile devices **must not** be kept with the device.

Unauthorised use of mobile devices puts SCRA's information at risk, and dependant on the type of device could compromise the SCOTS network.

Lost or stolen mobile devices **must** be reported immediately.

Data encryption of laptop's hard drives is only effective when the device is shut down so users must shut down the laptop when it is not in use. A laptop **must not** be transported in stand-by mode.

7.3 Definitions

7.3.1 Mobile Device

A portable device used for communication or for running applications, such as a laptop, tablet, mobile phone, smart phone, etc. Portable storage devices such as backup tapes, CD-ROMS, DVDs and memory sticks etc. are also included.

7.3.2 Smart Phones

These handheld wireless devices can access a range of information services including email, calendar, mobile telephone, text messaging, etc. There are two types of smart phone that are issued to authorised SCRA users, Apple's iPad or the Samsung smartphone[33].

7.3.3 Laptops

Networked Laptops

Laptops configured for direct connection to the SCOTS network are supported by SCOTS and their hard disk is encrypted. Although these laptops can be used for working offline, the user must have successfully logged on and off the SCRA network at least once beforehand. This is required so that the offline profile is stored on the laptop.

Users should shut down their laptop at the end of their working day and not just sign out.

This ensures that all files and applications are closed and any software updates, or system and application changes, are automatically applied to the user's laptop during the next restart.

[33] Please check with the SCRA IT Service Desk for the most up to date validated version of this device.

Un-networked Laptops

These laptops are not recognised by the SCOTS network and are configured specifically for offline work. These laptops are **not** to be used for long-term storage[34] of OFFICIAL–SENSITIVE classified data or personal data.

7.3.4 Mobile Device User

A mobile device user is any SCRA member of staff (or third party suppliers and contractors) issued with an SCRA mobile device or granted use of these devices.

7.3.5 Generic Passwords

A generic password is a password known only by a group of mobile device users allowing them access to shared devices (e.g. pool laptops, hearing laptops).

7.4 Responsibilities

7.4.1 User responsibility

All mobile device users must comply with this policy. Mobile devices are not only attractive objects to steal, but unauthorised use of the device puts both SCRA's information and the SCOTS network at risk.

Users are responsible for using any additional security devices (e.g. Kensington Lock) and any built in security controls (e.g. remote access software, BitLocker encryption) specifically set up to protect their mobile devices.

All users are responsible for the security of their mobile device at all times and in the event of their device being lost or stolen alerting the SCRA IT Service Desk (and if appropriate SCOTS, Finance section[35] and their network provider – see Loss or Theft).

Most mobile devices are provided with built-in security, users must not change these settings unless otherwise directed by the IT Team or iTECS.

7.4.2 The IT Team

The IT Team[36] are responsible for:-

- agreeing the general security configuration of mobile devices and maintaining records of these settings;
- the keeping of records on who (or which SCRA office) the mobile device is issued to and for maintaining records of generic passwords;
- providing guidance and advice to users on how to secure their mobile devices;
- the keeping of records relating to all security incidents, including loss and theft of mobile devices.

7.5 General Usage

Employees **must not** allow unauthorised use of their mobile devices; this includes family members, friends and associates.

Employees **must not** modify software supplied with the mobile device or install additional software.

[34] Short-term storage of personal data is allowed so hearing forms can be completed and printed.

[35] For mobile devices with an asset value.

[36] With respect to SCOTS assets, iTECS assists the IT Team with this responsibility.

7.5.1 Device Protection

Most mobile devices are protected by either a password or a personal identification number (PIN). Where possible[37], users are to comply with SCRA's Password Policy.

Users must be aware of shoulder surfers who try to watch as they enter their password into the device. If a user believes that their password has been compromised they should change it immediately.

7.5.2 Protecting Mobile Devices during Transit

Laptops

- If travelling by car, users **must** place laptops out of sight preferably in the vehicle's boot (or out of sight in an estate car) and should avoid leaving them unattended in the vehicle. If the laptop is left unattended in the vehicle, the vehicle **must** be locked, and laptops **must not** be left overnight in a vehicle.
- Keep passwords secure and separate from the laptop or laptop case.
- When staying in a hotel, the laptop, whilst not in use, should be stored in the hotel safe or if a Kensington Lock is provided, secured to an immovable object.
- Laptops must be carried as hand luggage when travelling by air, and kept in sight at all times whilst travelling on public transport.
- Do not view personal or sensitive information on your laptop when in public.
- Laptops must be powered down during transit or when not in use.

Other Mobile Devices

If the user is not intending on using these devices during transit then they **must** be switched off and kept out of site, either in the users clothing or in their hand luggage. Users **must not** leave their hand luggage unattended if it contains a mobile device.

7.5.3 Loss or Theft

In the event of a mobile device being lost or stolen, then the employee's manager and the IT Team **must** be notified immediately. If the device is stolen then the police **must** also be notified.

If an iPad or Samsung smartphone is lost or stolen, the user must get in touch with Vodafone immediately to let them know on 0333 304 3333 and then report this to the SCRA IT Service Desk.

Lost and stolen smartphones **must** be reported to iTECS **as soon as possible** so that 'secure bubble' can be remotely wiped.

Lost and stolen SCOTS laptops **must** be reported to iTECS.

If an employee's mobile device is stolen, and it is deemed that the necessary security precautions were not followed, e.g. use of security device, the Locality or Head Office team will be responsible for the cost of replacing the mobile device as well as any other associated costs in providing a new device.

[37] Some mobile devices may be configured by the manufacturer/supplier with their default password policy which cannot be changed or an alternative authentication process not complaint with SCRA's password policy.

7.6 Laptops

7.6.1 Networked Laptops

Laptop Usage

Users can configure their SCOTS laptops for off-line working – see the 'Offline files' section of the Remote Working –Tips & Troubleshooting guidance. Synchronisation of off-line and on-line folders is required each time you log on and log off SCOTS to ensure that the latest version of the document is available.

Physical Security

Kensington Locks are provided with networked laptops and users are to secure their laptop to an immovable object to discourage theft, especially when leaving their laptop in the office overnight. Where it is impractical to use the Kensington Lock, employees must keep the mobile device with them and use common sense to prevent against theft. There is no need to use a Kensington Lock when working from home as the home is a secure environment.

Access to SCOTS

Users must connect their laptop either directly into the SCOTS network using the Ethernet cable provided or remotely through a wireless connection using a SCOTS Laptop (e.g. using their home broadband or the OnSCOTS Wi-Fi available in SCRA offices). Users must not attempt to connect to SCOTS using web portals (e.g. as provided by a hotel) or using non-SCOTS procedures (e.g. BT Broadband access to the Internet).

Remote Access to SCRA systems

CSAS is a cloud-based service and all users gain access to CSAS using their SCOTS user account on their laptop and the CSAS login, this includes working from home.

SCRA allows staff to remotely access iTrent through SCOTS as part of the iTrent self-service. iTrent Admin users are allowed to access iTrent remotely through SCOTS, so that they are able to support iTrent.

eFinancials users are allowed to access the system remotely through SCOTS so that they are able to support eFinancials.

Regular Connection

Users **must** connect the laptop to the SCRA network regularly, preferably once a week for at least 60 minutes, but **at a minimum** once per month. The longer a laptop is disconnected from the SCOTS network then the higher the risk of the data on the laptop being compromised. Network connection allows the device to be updated with the latest anti-virus software and any other security patches deemed necessary by SCOTS. Regular connection is also required for data synchronisation between offline and networked folders.

7.6.2 Un-networked Laptops

Physical Security

Kensington Locks are provided with un-networked laptops and users **must** ensure that the laptop is secured to an immovable object to discourage theft.

7.7 iPads and Samsung Smartphones Usage

SCRA offers eligible colleagues with either an iPad or a Samsung smartphone. These corporate devices provide users access to SCOTS services created within a 'secure bubble' through a set of BlackBerry apps. Users can use their devices to access non-SCOTS provided services such as:-

- browsing the internet;
- installing and using personal business apps of their choice.

This model of service is termed 'Corporately Owned, Personally Enabled' – COPE.

SCRA defines acceptable business use as activities that directly or indirectly support SCRA's business. Users are to be familiar with the Mobile services employee agreement and usage must comply with this policy and the SCOTS IT Code of Conduct.

iTECS will support issues surrounding the installation and the synchronization of email/ calendar/ contacts within the 'secure bubble'.

SCRA staff are not to upgrade their device to the latest operating system (OS) until explicitly requested to do so by iTECS. This will allow the 'secure bubble' to be tested with any new OS. Any upgrade not tested may result in the service not working.

Users must seek guidance from the SCRA IT Service Desk if they intend to use their COPE devices overseas, this must be done at least 2 weeks before their trip.

Further guidance on the iPad and Samsung smartphone is available on Connect. Users should contact the SCRA IT Service Desk if they have any queries in relation to using these devices.

7.8 DVDs, CD-ROMS, Data Tapes, Secure Memory Sticks

All DVDs, CD-ROMS, data tapes, and secure memory sticks used to store SCRA information must be stored in locked cabinets when not in use. Use of locked carrying cases should be considered when travelling with these mobile devices.

7.9 Mobile Phones and Tablets

These devices do not use disk encryption so must not to be used for storing personnel or OFFICIAL–SENSITIVE data for business reasons. Users storing their own personnel data on these devices must be aware of the risks they are taking as these devices are only protected by a password or a Personnel Identification Number (PIN).

8 Data Classification Policy

Version 1.3 24 September 2021

8.1 Purpose

This policy defines the security classifications in use by SCRA to identify information (or other specific assets) of different sensitivities and how to protectively mark sensitive information assets. It also defines the protection measures required for safeguarding classified and protectively marked information whether this is SCRA's information or a business partner's information received through a data sharing agreement or Memorandum of Understanding (MOU).

8.2 Key Principles

By adopting the Cabinet Office's Government Security Classification Policy, SCRA's key principles are:-

- All information that SCRA collects, stores, processes, generates or shares in order to perform their role has intrinsic value and is to be appropriately protected.
- Everyone who works within SCRA (including staff, consultants and agency workers) has a duty of confidentiality and a responsibility to safeguard any SCRA information or data that they have access to, irrespective of whether it is marked or not.
- Access to **sensitive** information is to be granted on a genuine 'need to know' basis.
- Information received from or exchanged with external partners is to be protected in accordance with relevant legislative or regulatory requirements.

8.3 Definitions

8.3.1 Government Security Classifications (GSC)

The Government Security Classifications offer three levels of classification:-

- TOP SECRET
- SECRET
- OFFICIAL

The majority of information that is created or processed by the public sector is to be classified at the OFFICIAL level, some of which could have damaging consequences if lost stolen or published in the media, but are not subject to a heightened threat profile.

OFFICIAL–SENSITIVE is a subset of the OFFICIAL classification which is to be used for particularly sensitive information and should be managed within the OFFICIAL classification tier.

8.3.2 Protective Marking using GSC

For particularly sensitive information requiring a more limited 'need to know', level of protection then a **caveat** is used by protectively marking the information as **OFFICIAL–SENSITIVE**.

There is no requirement to explicitly mark routine OFFICIAL information.

8.3.3 Handling Descriptors using GSC

Applying a **handling descriptor** to the protective marking makes the need for protection clearer, for example when adding the handling descriptor to the **OFFICIAL–SENSITIVE** protective marking. There are 2 descriptors that are currently in use by SCRA, these are:-

- COMMERCIAL – commercial or market sensitive information
- PERSONAL – sensitive information relating to an identifiable individual

e.g. OFFICIAL–SENSITIVE PERSONAL

8.4 Responsibilities

8.4.1 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for the implementation of the Government Security Classifications and for defining the data handling requirements for classified data. The SIRO appoints Information Asset Owners to control their own information assets and is responsible for investigating breaches of classified information assets.

8.4.2 Staff responsibility

All staff are to set up an OFFICIAL–SENSITIVE PERSONAL email signature in accordance with the Protective Marking Emails guidance issued on Connect. Staff are expected to understand the data classification policy and how it applies to the information assets that they handle.

8.4.3 Information Asset Owner (IAO)

The Information Asset Owner (IAO) is responsible for the classification of their information assets. The IAO leads and fosters a culture within SCRA so that the key principles of the data classification policy are met.

8.5 Classification of SCRA's information

Apart from information that is publicly available, all SCRA's information is classified at the OFFICIAL level. SCRA does not work with information classified at the SECRET or TOP SECRET levels.

SCRA's general business information falls within the OFFICIAL classification.

Table 2 shows the difference between general business information and when the information is sensitive requiring added protection. Due to the nature of SCRA's business SCRA regards all personal information as OFFICIAL–SENSITIVE.

OFFICIAL	It becomes OFFICIAL–SENSITIVE when…
All records which allow people to be identified are "personal data" and we are trusted to protect it.	…children or vulnerable adults may be at direct risk of harm if the information is shared with the wrong people.
Management information and reports are critical to smooth running and accountability of the business.	…announcements or processes associated with it would be seriously harmed if released.
Draft reports are protected before released to the public.	…the content is so controversial that mishandling will have serious consequences for SCRA or Scottish Government.
Information Technology network plans might be commercially sensitive or contain details of security controls in place.	…it indicates our security vulnerabilities which allows an attacker the opportunity to seriously compromise our systems.
Policy development and advice to ministers.	…if the subject is very contentious and sensitive

Table 2: Routine business information and sensitive business information

8.6 Protective Marking of SCRA's information

There is no requirement to explicitly mark routine OFFICIAL information.

All personal information is sensitive, so when sending case or staff information electronically (i.e. communications with social work, etc.) the email **must** be protectively marked as:-

OFFICIAL–SENSITIVE PERSONAL

All staff dealing regularly with case information must set up their default signature so emails are marked OFFICIAL–SENSITIVE PERSONAL.

When the information being sent by email is not sensitive, staff should select a more appropriate email signature for the communication being sent, or remove their default signature completely before drafting the email.

Staff that send **non-personal sensitive** information to Scottish Government, partner organisations or suppliers through emails are to protectively mark them as either:-

OFFICIAL–SENSITIVE or **OFFICIAL–SENSITIVE COMMERCIAL**

whichever is appropriate to the information being sent.

Staff using these protective markings regularly should set up their email signatures, using the guidance, so these markings can be selected when additional protection is needed.

8.7 Other Classification schemes

Care must be taken when receiving information that is classified to another classification scheme (e.g. NHS) to ensure the information is adequately protected. Staff receiving documents marked to another classification scheme should contact Digital Security and Governance (DS&G) Manager to find out how this information should be handled.

Staff revising a document that was previously protectively marked using the Government Protective Marking System (GPMS)[38] must replace the marking with the GCS equivalent classification. The old markings such as NON–PROTECTIVELY MARKED, UNCLASSIFIED or PROTECT must be removed as these fall within the OFFICIAL classification. Documents marked RESTRICTED are now to be marked as OFFICIAL–SENSITIVE.

8.8 Handling of Classified Data

All of SCRA's classified information is at the OFFICIAL level, and any classified information that SCRA receive from business partners is also classified at the OFFICIAL level (or the OFFICIAL equivalent). SCRA does not handle information classified as SECRET or TOP SECRET.

Appendix C defines the handling arrangements for OFFICIAL classified information and what additional protective measures are to be applied for OFFICIAL–SENSITIVE classified information.

8.8.1 Case Information

Although all case information is classified as OFFICIAL–SENSITIVE information, often reports are not marked as such, for various business reasons. Staff working with case information that is not marked must apply the data handling measures for OFFICIAL–SENSITIVE information.

Local procedures have been put in place for staff to follow when they need to take case information out of the office.

See SCRA's Data Protection Policy for further detail on protecting SCRA's case information.

[38] GPMS was replaced by GSC in April 2014.

9 eFinancials Security Policy

Version 2.4 24 September 2021

eFinancials Security Policy Context

eFinancials is a financial and management accounting system and the core eFinancials application has 5 components:-

eAnalyser – an interrogating tool.
Web CoA – web application that allows amending the Chart of Accounts (CoA).
Xcel Uploader – uploading facility to import data out of MS Excel.
DbCapture – an imaging tool for creditor payments stored in pdf format.
FPM – Finance Process Manager data entry, routing an approvals application.

eFinancials is a client / server application using secure web technologies to provide access to all SCRA's financial records such as transactions, budgets, etc. Furthermore, the eFinancials system also processes information provided by other agencies. Consequently, it is important that staff working on the eFinancials system:-

- Comply with current legislation;
- Adhere to SCRA security policies;
- Use the system in an acceptable way and only for intended business purposes;
- Do not create unnecessary business risk or reputational damage to the SCRA by their misuse of the eFinancials system or the data it provides access to.

SCRA currently provides shared services to Children's Hearings Scotland (CHS), administering their Accounts Payable (AP) function and payroll payments.

Overarching Policy Statements

- Administration access to the eFinancials system is permitted to authorised SCRA users for legitimate business purposes only. Under no circumstances can the system be used for non-financial and non-management related activity or for personal browsing;
- SCRA Staff should be aware that activity undertaken on the eFinancials system is subject to monitoring and that mechanisms are in place to identify inappropriate activity;
- SCRA has a 'duty of care' with regard to the safekeeping of financial information and has a statutory requirement to produce accounts. SCRA Staff must be supportive of these obligations through compliance with this and the wider SCRA Information Security Policy Set;
- Under no circumstances should staff share access rights to the eFinancials system or disclose their access credentials to anyone. Activities undertaken through a named user account are directly attributable to that individual;
- All users of the eFinancials system must be aware of their obligations towards the Computer Misuse Act and ensure full compliance with this.

Policy Objectives

SCRA staff should at all times, conduct themselves honestly and appropriately when using the eFinancials system and in particular must not: -

- Place at risk the integrity, security or operation of eFinancials system or the equipment used to facilitate access to it;
- Engage in any action or activity, which would place themselves as individuals or SCRA, liable to criminal prosecution or civil action;
- Access eFinancials data for anything other than its intended business purpose;
- Transmit eFinancials data via unsecured/non-approved channels (e.g. to non-secure email addresses);
- Allow unauthorised access to the eFinancials system or disclosure of the data it stores;
- Engage in any action, which would bring SCRA into disrepute.

9.1 Section 1 – Introduction

9.1.1 Scope

This policy provides guidance to SCRA staff on the appropriate usage of eFinancials and its components. It applies to only SCRA employees with a SCOTS user account and approved contractors working on behalf of SCRA that have been granted access to the eFinancials system. SCRA employees includes:-

- Those in full time or part time employment on fixed term or permanent contracts within SCRA;
- Those employees on secondment into or from SCRA (subject to terms and conditions of the secondment arrangement).

For the purpose of this policy, the term "SCRA staff" refers to all approved personnel including consultants. However, this term is not intended to determine employee status.

For the purpose of this policy, the term "eFinancials" refers to eFinancials and all its components.

9.1.2 eFinancials Usage

eFinancials is a financial and management accounting system supplied, maintained and supported under contract with Advanced (formerly "Advanced Business Solutions"). As such eFinancials provides access to SCRA's financial and management records under the jurisdiction of the SCRA. Furthermore, the eFinancials system also processes information provided by other agencies. Consequently it is important that SCRA staff working on the eFinancials system are made aware of, and comply with, all relevant information security policies and wider legislative obligations.

Full copies of this policy, other SCRA security policies, guidelines and a link to the SCOTS IT Code of Conduct are all available on Connect.

9.1.3 Benefits

eFinancials is a valuable business tool and delivers improved service delivery and efficiencies in processing. However, misuse of this facility and inappropriate handling of sensitive financial data can lead to significant reputational damage and financial penalties for SCRA and CHS.

The purpose of this policy is primarily to reduce the risk of unauthorised access, loss of, and damage to the financial and management information held within eFinancials.

9.1.4 Ownership and Authority

The Policy is owned and managed by the Head of Finances and Resources, as Financial Information Asset Owner (IAO), with support from:

- the Digital Security and Governance (DS&G) Manager for guidance on information security policy matters;
- the Information Governance Officer (IGO) for guidance on data protection matters;
- the Finance Team.

The Head of Finances and Resources is responsible for ensuring that SCRA staff are aware of and adhere to this Policy.

The consequences for SCRA and individuals of inappropriate disclosure of information could be severe, disruptive and demoralising. If you have any questions regarding any aspect of this Policy you should, in the first instance, raise them with your line manager.

9.1.5 Roles and Responsibilities

eFinancials users are responsible for the maintaining the confidentiality and integrity of all records that they access in accordance with this policy.

eFinancials System Administrators are responsible for:-

- assigning access permissions once they have been approved;
- maintaining the confidentiality and integrity of all records that they access in accordance with this policy;
- setting up audit logs and reviewing logs regularly.

The Head of Finances and Resources is responsible for approving all changes in user access ensuring that it is commensurate with that SCRA staff's role. The Head of Finances and Resources is also responsible for ensuring that new users of eFinancials are aware of this policy and for ensuring that it is understood.

9.1.6 Policy Review

The Head of Finances and Resources with the assistance of the DS&G Manager will review and evaluate the effectiveness of this policy in line with legal and statutory requirements. The policy may be withdrawn or amended in accordance with these review procedures. Staff are encouraged to feedback any comments or issues encountered when applying this policy.

9.1.7 Financial Audit

SCRA is fully committed to keeping accurate financial records as it is accountable to Scottish Government for expenditure against yearly budgets and its accounts are audited annually. In order to efficiently carry out its business, SCRA must collect and use financial and management information, which it does through eFinancials.

9.1.8 Emailing from eFinancials

There is no facility for users to email directly from eFinancials.

9.2 Section 2 – The Policy

9.2.1 Introduction

Given the commercially sensitive nature of the finance and management records, SCRA must not find itself discredited or undermined by any thoughtless or ill-informed action on the part of its staff.

9.2.2 Reasons for this Policy

All information generated by SCRA or given into safekeeping by any third party must be adequately protected against breach of confidentiality, loss of integrity and loss of availability. It is important that SCRA can demonstrate that they are a safe custodian of data. It is therefore important that there is a clearly stated policy on the use of the eFinancials system, to explain what is or is not acceptable.

9.2.3 Access

Access to eFinancials requires having both a SCRA SCOTS user account and an eFinancials user account. All new SCRA staff must obtain full Baseline Personnel Security Standard (BPSS) clearance as a prerequisite to obtaining a SCOTS user account. All SCRA staff are required to familiarise themselves with the SCOTS IT Code of Conduct which all SCOTS users agree to abide to during the SCOTS log in process.

Four levels of access are accommodated within eFinancials:-

- Transaction user accounts provide access for recording and reviewing financial transactions;
- Business Team user accounts provide limited access so expenditure can be checked against budgets in the users own area of business;
- Finance user accounts provide full access to eFinancials records;
- System administration accounts have full access to all eFinancials records and can assign access permissions to other eFinancials user accounts.

Usually access to eFinancials is made through a direct connection into the SCOTS network using SCOTS equipment, i.e. staff obtain access through their desktops/laptops within an SCRA office. Remote access to eFinancials through an SCRA laptop is allowed through the use of a Virtual Private Network (VPN). Access to eFinancials through an internet connection is not allowed and has been disabled.

9.2.4 User Authentication

The eFinancials system requires a valid user ID and password to be entered into the eFinancials login screen before access to the systems is obtained. eFinancials enforces the user to select a strong password and to change their password regularly in order to protect against unauthorised access.

The following password rules are to be applied:-

- Passwords must be at least eight characters in length and contain a mixture of upper-case letters, lower-case letters, and numbers;
- Avoid using passwords which have user significance and which could be easily guessed (e.g. 'password', login name, user name, dates of birth, car make/model/registration, family or relation names, football teams/player, etc.);
- Passwords must be changed regularly, at least every twelve months and should not be recycled;
- Passwords must not be made known to anyone else and changed if it is suspected that they have become known;
- If, in exceptional circumstances, there is a need to write a password down, then it should be stored securely in locked furniture or office safe.

Under no circumstances should staff share access rights to the eFinancials system or disclose their access credentials to anyone. Activities undertaken through a named user account are directly attributable to that individual.

9.2.5 Data Entry

Personal information is not to be entered into eFinancials, but if the transaction relates to a personal expense then the employees staff number should be entered instead, or alternatively the persons initials.

9.2.6 Handling of Records

All eFinancials records are commercially sensitive and use the Government Security Classification caveat - OFFICIAL–SENSITIVE. All printouts from the system containing commercial data must be marked OFFICIAL–SENSITIVE COMMERCIAL and handled appropriately to this classification, that is:-

- stored within a secure building in a locked container;
- disposed as confidential waste;
- fax may not be used.

eFinancials records can only be transmitted by email to addresses that are known to belong to a secure domain such as the SCOTS domain (gov.scot), the CJSM domain (cjsm.net and other approved email domains. If there is a need to send eFinancials records electronically to other environments then the DS&G Manager must be informed so the need can be assessed and appropriate encryption applied. Communications are to be sent to individuals on the 'need to know' principle.

9.2.7 User Activity Monitoring

User activity on the eFinancials system is logged for system maintenance, audit and performance reasons and may be seen by the system administrator in the course of their duty. Inappropriate usage is to be identified and reported. SCRA has a range of statutory and legal responsibilities and staff who are found to have breached these obligations will be subject to all appropriate measures including, where necessary, criminal prosecution.

User activities within the eFinancials system will be monitored in accordance with relevant legislation to investigate actual, apparent or alleged misuse, improper behaviour, internal or external attacks, security issues or other similar incidents.

9.2.8 Use of the Search Facility

The eFinancials system 'search facility' is provided only for legitimate business purposes. Under no circumstances should this facility be misused for any non-business requirement. Audit and monitoring arrangements are in place to monitor the use of this facility and any unusual activity will be investigated. Staff identified as being engaged in inappropriate use of the search facility or indeed any other element of the eFinancials system will be subject to disciplinary action.

9.2.9 Discussions relating to eFinancials Data

SCRA Staff must take care when discussing financial details when accessing an eFinancials record. Before discussions take place via telephone, staff should take steps to validate the identity of the person they are talking to. If any doubts exist, financial information should not be disclosed and further confirmation must be sought. Staff must not discuss financial and management information in public places and should ensure that when meetings take place, that these cannot be overheard.

9.2.10 Training Data

The live eFinancials system must not be used as a training system and no false or training data should be loaded on to this system. The eFinancials Test system is to be used for user training.

9.2.11 System Configuration

Users must not attempt to make changes to the system configuration, including connections to external systems and communications facilities. SCRA IT infrastructure from which access to eFinancials is made, is managed by Information and Technology Services Division (iTECS), and any installation of eFinancials software on the SCOTS systems is iTECS responsibility. eFinancials server configuration is the responsibility of Advanced.

9.2.12 System Availability

Service level agreements are in place with Advanced to ensure that essential eFinancials services are restored quickly. If eFinancials is unavailable and no communication has been received to indicate why it is offline, then the fault should be reported to the System Administrator.

In the event that the incursion of malicious software or other malicious activity is discovered during an authenticated session on eFinancials, the following precautions are to be taken to quarantine the system until further advice has been obtained:-

- Refrain from all further processing;
- Inform your line manager;
- Contact the SCOTS IT Helpdesk on Ext 48500

9.2.13 Incident Management

Users must familiarise themselves with SCRA's guidance on phishing so that SCRA can minimise their exposure to this potential threat.

Any user who becomes aware of, or has reason to suspect a vulnerability or incident of potential security significance must follow the SCRA Incident Management Procedure.

9.2.14 Compliance with Legal Requirements

All users must familiarise themselves with their obligations to comply with relevant legislation and regulations.

Disclosure of Information

The legislation governing the authorised or unauthorised disclosure of information includes the following:-

- Public Records (Scotland) Act 2011;
- Data Protection Act 2018;
- Freedom of Information (Scotland) Act 2002;
- Human Rights Act 1998.

Computer Misuse Act 1990

All users are to be aware of the legal requirements of the Computer Misuse Act 1990, a summary of which follows.

Section 1: Unauthorised Access to Computer Material

It is an offence knowingly to cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer. The underlying intent need not be directed at any particular program or data, or at a program or data of any particular kind, which is held in any particular computer. Nor has any change to the program or data occurred as a result of the access. Thus unauthorised "browsing" through a program or data, or an attempted access, even if unsuccessful, is an offence, as is the access by authorised staff who knowingly exceed or attempt to exceed their defined level of access authorisation.

Section 2: Unauthorised Access with Intent to Commit or Facilitate Commission of further Offences

It is an offence, if an offence under section 1 (above) is committed with the intent to commit or facilitate a further offence by the offender or any other person. Actual damage need not result, and it is immaterial whether the further offence is committed or even possible.

Section 3: Unauthorised Modification of Computer Material

It is an offence intentionally to do any act, which causes an unauthorised modification of the contents of any computer, to prevent or hinder access to any program or data held, or to impair the operation of the program or the reliability of the data. This includes the infection of any system with malicious software.

9.2.15 Breach of Policy

Investigation and Disciplinary Action

Disciplinary action may be taken in accordance with the SCRA Disciplinary Policy and Procedures and may result in dismissal. Staff should also be aware that findings on an investigation might lead to criminal proceedings in certain instances.

Questions relating to any aspect of this Policy should be raised via line managers or with the Digital Security and Governance (DS&G) Manager .

10 iTrent System Security Policy

Version 1.5 24 September 2021

iTrent Security Policy Context

The iTrent system is a Payroll and Human Resource (HR) information management system. As such, it provides access to an extensive range of sensitive information on SCRA and Children's Hearings Scotland (CHS) employees under the jurisdiction of SCRA. Furthermore, the iTrent system also processes information provided by other agencies. Consequently, it is important that staff working on the iTrent system:-

- Comply with current legislation;
- Adhere to SCRA security policies;
- Use the system in an acceptable way and only for intended business purposes;
- Do not create unnecessary business risk or reputational damage to the SCRA by their misuse of the iTrent system or the data it provides access to.

Overarching Policy Statements

- Administration access to the iTrent system is permitted to authorised SCRA users for legitimate business purposes only. Under no circumstances can the system be used for non-HR and non-Payroll related activity or for personal browsing;
- SCRA Staff with access to the SCOTS network have access to their own iTrent records (iTrent self-service) and are responsible for maintaining the accuracy and confidentially of their own information;
- SCRA Staff should be aware that activity undertaken on the iTrent system is subject to monitoring and that mechanisms are in place to identify inappropriate activity;
- SCRA has a 'duty of care' with regard to the safekeeping of sensitive information and has obligations under legislation such as the Data Protection Act 2018 in relation to personal data. SCRA Staff must be supportive of these obligations through compliance with this and the wider SCRA Information Security Policy Set;
- Under no circumstances should staff share access rights to the iTrent system or disclose their access credentials to anyone. Activities undertaken through a named user account are directly attributable to that individual.
- All users of the iTrent system must be aware of their obligations towards the Computer Misuse Act and ensure full compliance with this.

Policy Objectives

SCRA staff should at all times, conduct themselves honestly and appropriately when using the iTrent system and in particular must not: -

- Place at risk the integrity, security or operation of iTrent system or the equipment used to facilitate access to it;
- Engage in any action or activity, which would place themselves as individuals or SCRA, liable to criminal prosecution or civil action;
- Access iTrent data for anything other than its intended business purpose;
- Transmit iTrent data via unsecured/non-approved channels (e.g. to non-secure email addresses);
- Allow unauthorised access to the iTrent system or disclosure of the data it stores;
- Engage in any action, which would bring SCRA into disrepute.

10.1 Section 1 – Introduction

10.1.1 Scope

This policy provides guidance to SCRA staff on the appropriate usage of the iTrent system. It applies to only SCRA employees with a SCOTS user account and approved contractors working on behalf of SCRA that have been granted access to the iTrent system. SCRA employees includes:-

- Those on fixed term or permanent contracts within the SCRA;
- Those employees on secondment into or from SCRA (subject to terms and conditions of the secondment arrangement).

For the purpose of this policy, the term "SCRA staff" refers to all approved personnel including consultants. However, this term is not intended to determine employee status.

10.1.2 iTrent Usage

The iTrent system is a Payroll and Human Resource (HR) information management system supplied under contract with Insight but maintained and supported by MidlandHR. As such, iTrent provides access to an extensive range of sensitive information that is under the jurisdiction of the SCRA. Furthermore, the iTrent system also processes information provided by other agencies. Consequently, it is important that SCRA staff working on the iTrent system are aware of, and comply with, all relevant information security policies and wider legislative obligations.

iTrent self-service provides all SCRA staff with SCOTS user accounts access to their own HR and Payroll records so accuracy of these records can be maintained.

Full copies of this policy, other SCRA security policies, guidelines and a link to the SCOTS IT Code of Conduct are all available on Connect.

10.1.3 Benefits

iTrent is a valuable business tool and delivers improved service delivery and efficiencies in processing. However, misuse of this facility and inappropriate handling of sensitive and/or personal data can lead to significant reputational damage and financial penalties for SCRA. Inappropriate use of iTrent could have serious consequences for the SCRA and the CHS employees that SCRA deals with.

The purpose of this policy is primarily to reduce the risk of unauthorised access, loss of, and damage to the personal information held within iTrent.

10.1.4 Ownership and Authority

The Policy is owned and managed by the Head of Human Resources, as HR and Payroll Information Asset Owner (IAO), with support from:-

- the Digital Security and Governance (DS&G) Manager for guidance on information security policy matters;
- the Information Governance Officer (IGO) for guidance on data protection matters;
- the HR and Payroll Teams.

The Head of Human Resources is responsible for ensuring that SCRA staff are aware of and adhere to this policy.

The consequences for SCRA and individuals of inappropriate disclosure of information could be severe, disruptive and demoralising. If you have any questions regarding any aspect of this policy you should, in the first instance, raise them with your line manager.

10.1.5 Roles and Responsibilities

All SCRA staff with SCRA user accounts are responsible for maintaining the accuracy and confidentially of their own iTrent information through iTrent self-service.

iTrent Administrators are responsible for maintaining the confidentiality and integrity of all records that they access in accordance with this policy.

ITrent System Administrators are responsible for:-

- assigning access permissions once they have been approved;
- maintaining the confidentiality and integrity of all records that they access in accordance with this policy;
- setting up audit logs and reviewing logs regularly.

The Head of Human Resources is responsible for approving all changes in user access ensuring that it is commensurate with that SCRA employee's role.

It is the responsibility of all SCRA staff to ensure that this policy is implemented within the areas of their responsibility or control. When new staff are recruited, their line manager is responsible for drawing attention to this policy and for ensuring it is understood.

10.1.6 Policy Review

The Head of Human Resources with the assistance of the DS&G Manager will review and evaluate the effectiveness of this policy in line with SCRA's legal and statutory requirements. The policy may be withdrawn or amended in accordance with these review procedures. Staff are encouraged to feedback any comments or issues encountered when applying this policy.

10.1.7 Data Protection

In order to efficiently carry out its business, SCRA must collect and use information on their employees. In order for SCRA to provide an HR and Payroll service to CHS, SCRA collects and uses information on CHS employees too. All information collected will be processed in accordance with data protection laws.

10.1.8 Data Sharing

Most SCRA and CHS staff contribute to the Local Government Pension Scheme run by Falkirk Council and Lothian Council respectively and sensitive pension information is recorded on ITrent. Routine reports for pension purposes are produced using iTrent and shared with Falkirk Council Pension Department as part of an on-going agreement between SCRA and Falkirk Council Pension Department. SCRA also share personal sensitive information with Optima Health, SCRA's Occupational Health provider. We seek consent with the individual employee in the first instance to share the information and an appropriate data sharing agreement is in place as part of the ongoing contractual arrangements.

10.1.9 Emailing from iTrent

There is no facility for users to email directly from iTrent. When a member of staff makes a change to their own record using iTrent self-service then the system generates an email to the appropriate authority to advise that a change has been made.

10.2 Section 2 – The Policy

10.2.1 Introduction

Given the sensitive nature of the HR and payroll records, SCRA must not find itself discredited or undermined by any thoughtless or ill-informed action on the part of its staff.

10.2.2 Reasons for this Policy

All information generated by SCRA or given into safekeeping by any third party must be adequately protected against breach of confidentiality, loss of integrity and loss of availability. It is important that SCRA is demonstrated to be a safe custodian of data. It is therefore important that there is a clearly stated policy on the use of the iTrent system, to explain what is or is not acceptable.

10.2.3 Access

Access to iTrent requires having both a SCRA SCOTS user account and an iTrent user account. All new SCRA staff must obtain full Baseline Personnel Security Standard (BPSS) clearance as a prerequisite to obtaining a SCOTS user account. All SCRA staff are required to familiarise themselves with the SCOTS IT Code of Conduct which all SCOTS users agree to abide to during the SCOTS log in process.

Three levels of access are accommodated within iTrent:-

- Self-service accounts have been created for all SCRA employees with a SCOTS user account and this provides access to their own iTrent records;
- Administration accounts have limited access and/or limited permissions with respect to iTrent records;
- System administration accounts have full access to all iTrent records and can assign access permissions to iTrent accounts.

Access to iTrent can only be made through the SCOTS network using SCOTS equipment. Staff can obtain access to iTrent within an SCRA office as their desktops/laptops are physically connected into the SCOTS network. SCRA staff issued with SCOTS laptops can access iTrent remotely. Access to iTrent using non-SCOTS equipment is disabled and if access is made this must be reported to the DS&G Manager as a security incident.

10.2.4 User authentication

The iTrent system requires a valid user ID and password to be entered into the iTrent login screen before access to the systems is obtained. iTrent enforces the user to select a strong password and to change their password regularly in order to protect against unauthorised access.

The following password rules must be applied:

- Passwords must be at least eight characters in length and contain a mixture of upper-case letters, lower-case letters, and numbers;
- Avoid using passwords which have user significance and which could be easily guessed (e.g. 'password', login name, user name, dates of birth, car make/model/registration, family or relation names, football teams/player, etc.);
- Passwords must be changed regularly, at least every twelve months and should not be recycled;
- Passwords must not be made known to anyone else and changed if it is suspected that they have become known;
- If, in exceptional circumstances, there is a need to write a password down, then it should be stored securely in locked furniture or office safe.

Under no circumstances should staff share access rights to the iTrent system or disclose their access credentials to anyone. Activities undertaken through a named user account are directly attributable to that individual.

10.2.5 User Activity Monitoring

User activity on the iTrent system is logged for system maintenance, audit and performance reasons and may be seen by the system administrator in the course of their duty. Inappropriate usage is to be identified and reported. SCRA has a range of statutory and legal responsibilities and staff who are found to have breached these obligations will be subject to all appropriate measures including, where necessary, criminal prosecution.

User activities within the iTrent system will be monitored in accordance with relevant legislation to investigate actual, apparent or alleged misuse, improper behaviour, internal or external attacks, security issues or other similar incidents.

10.2.6 Handling of records

All iTrent records are personal sensitive and use the Government Security Classification caveat - OFFICIAL–SENSITIVE. All printouts from the system containing personal data must be marked OFFICIAL–SENSITIVE PERSONAL and handled appropriately to this classification, that is:-

- stored within a secure building in a locked container;
- disposed as confidential waste;
- fax may not be used.

iTrent records can only be transmitted by email to addresses that are known to belong to a secure domain such as the SCOTS domain (gov.scot), the CJSM domain (cjsm.net) and other approved email domains. If there is a need to send iTrent records electronically to other environments then the DS&G Manager must be informed so the need can be assessed and appropriate encryption applied. Communications are to be sent to individuals on the 'need to know' principle.

10.2.7 Use of the Search Facility

The iTrent system 'search facility' is provided only for legitimate business purposes. Under no circumstances should this facility be misused for any non-business or personal browsing requirement. Audit and monitoring arrangements are in place to monitor the use of this facility and any unusual activity will be investigated. Staff identified as being engaged in inappropriate use of the search facility or indeed any other element of the iTrent system will be subject to disciplinary action.

10.2.8 Discussions relating to iTrent Data

SCRA Staff must take care when discussing other employee's personal details when accessing an iTrent record. Before discussions take place via telephone, staff should take steps to validate the identity of the person they are talking to. If any doubts exist, personal information should not be disclosed and further confirmation must be sought. Staff must not discuss employee's personal information in public places and should ensure that when meetings take place, that these cannot be overheard.

10.2.9 Training Data

The live iTrent system must not be used as a training system and no false or training data should be loaded on to this system. The iTrent Test system is to be used for user training.

10.2.10 System Configuration

Users must not attempt to make changes to the system configuration, including connections to external systems and communications facilities. SCRA IT infrastructure, from which access to iTrent is made, is managed by Information and Technology Services Division (iTECS), and

any installation of iTrent software on the SCOTS systems is an iTECS responsibility. ITrent system configuration is the responsibility of MidlandHR.

10.2.11 System Availability

Service level agreements (SLAs) are in place with MidlandHR to ensure that essential ITrent services are restored quickly. If iTrent is unavailable and no communication has been received to indicate why iTrent is offline then the fault should be reported to the SCRA's IT Team.

In the event that the incursion of malicious software or other malicious activity is discovered during an authenticated session on iTrent, the following precautions are to be taken to quarantine the system until further advice has been obtained:-

- Refrain from all further processing;
- Inform your line manager;
- Contact the SCOTS IT Helpdesk on Ext 48500.

10.2.12 Incident Management

Users must familiarise themselves with SCRA's guidance on phishing so that SCRA can minimise their exposure to this potential threat.

Any user who becomes aware of, or has reason to suspect vulnerability or an incident of potential security significance must immediately inform the DS&G Manager following existing SCRA incident management procedures.

10.2.13 Compliance with Legal Requirements

All users must familiarise themselves with their obligations to comply with relevant legislation and regulations.

Disclosure of Information

The legislation governing the authorised or unauthorised disclosure of information includes the following:

- Public Records (Scotland) Act 2011;
- Data Protection Act 2018;
- Freedom of Information (Scotland) Act 2002;
- Human Rights Act 1998.

Computer Misuse Act 1990

All users are to be aware of the legal requirements of the Computer Misuse Act 1990, a summary of which follows.

Section 1: Unauthorised Access to Computer Material

It is an offence knowingly to cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer. The underlying intent need not be directed at any particular program or data, or at a program or data of any particular kind, which is held in any particular computer. Nor need any change to the program or data have occurred as a result of the access. Thus unauthorised "browsing" through a program or data, or an attempted access, even if unsuccessful, is an offence, as is the access by authorised staff who knowingly exceed or attempt to exceed their defined level of access authorisation.

Section 2: Unauthorised Access with Intent to Commit or Facilitate Commission of further Offences

It is an offence if an offence under section 1 is committed with the intent to commit or facilitate a further offence by the offender or any other person. Actual damage need not result, and it is immaterial whether the further offence is committed or even possible.

Section 3: Unauthorised Modification of Computer Material

It is an offence intentionally to do any act, which causes an unauthorised modification of the contents of any computer, to prevent or hinder access to any program or data held, or to impair the operation of the program or the reliability of the data. This includes the infection of any system with malicious software.

10.2.14 Breach of Policy

Investigation and Disciplinary Action

Failure to comply with the rules set out in this policy may result in legal claims against you and SCRA and/or may lead to SCRA taking disciplinary action against you.

Potential breaches of the policy may be identified through either routine access and monitoring procedures (alerted to the DS&G Manager) or by an alert from an SCRA Manager. Any potential breaches will be investigated fully to ascertain if a breach has occurred and the relevant part of the policy/policies breached.

Disciplinary action may be taken in accordance with the SCRA Disciplinary Policy and Procedures and may result in dismissal. Staff should also be aware that findings on an investigation might lead to criminal proceedings in certain instances.

Questions relating to any aspect of this policy should be raised via line managers or with the Digital Security and Governance (DS&G) Manager.

11 Other System Security Policies and Guidance

Version 1.0 24 September 2021

11.1 Core System and Applications Solution (CSAS)

The Core System and Applications Solution (CSAS) has its own set of security policies and procedures, all of which are marked as OFFICIAL-SENSITIVE documents. As CSAS is a cloud application, it is accessible through the internet. There are various threat actors eager to gain access to public sector systems, such as CSAS, to fulfil their own goals, which is why the added protection is required.

By maintaining the Information Security Handbook as an OFFICIAL document allows it to be circulated more freely, for example to job applicants that have been offered a post in SCRA.

SCRA employees that need access to CSAS to perform their role, are required to sign a declaration agreeing to comply with both the CSAS Security Policy and CSAS SyOps.

There is a CSAS section in the Information Governance Library on Connect containing all the security policies and guidance relevant to CSAS users, such as the CSAS Security Monitoring Policy.

11.2 Remote Attendance Virtual Hearing Interface (RAVHI)

RAVHI has been designed specifically to protect Hearing Information Pack (HIP) data and personal data relating to those invited to attend virtual hearings. RAVHI has been built using MS cloud technologies and only SCRA's Virtual Hearings Team have user accounts on RAVHI.

All RAVHI users are required to sign the user declaration in the RAVHI SyOps, and by doing so they agree to comply with both the RAVHI Security Policy and the RAVHI SyOps. Both these documents are marked as OFFICIAL-SENSITIVE documents to ensure they are afforded additional protection.

12 Information Security Document Road Map

Version 1.2 24 September 2021

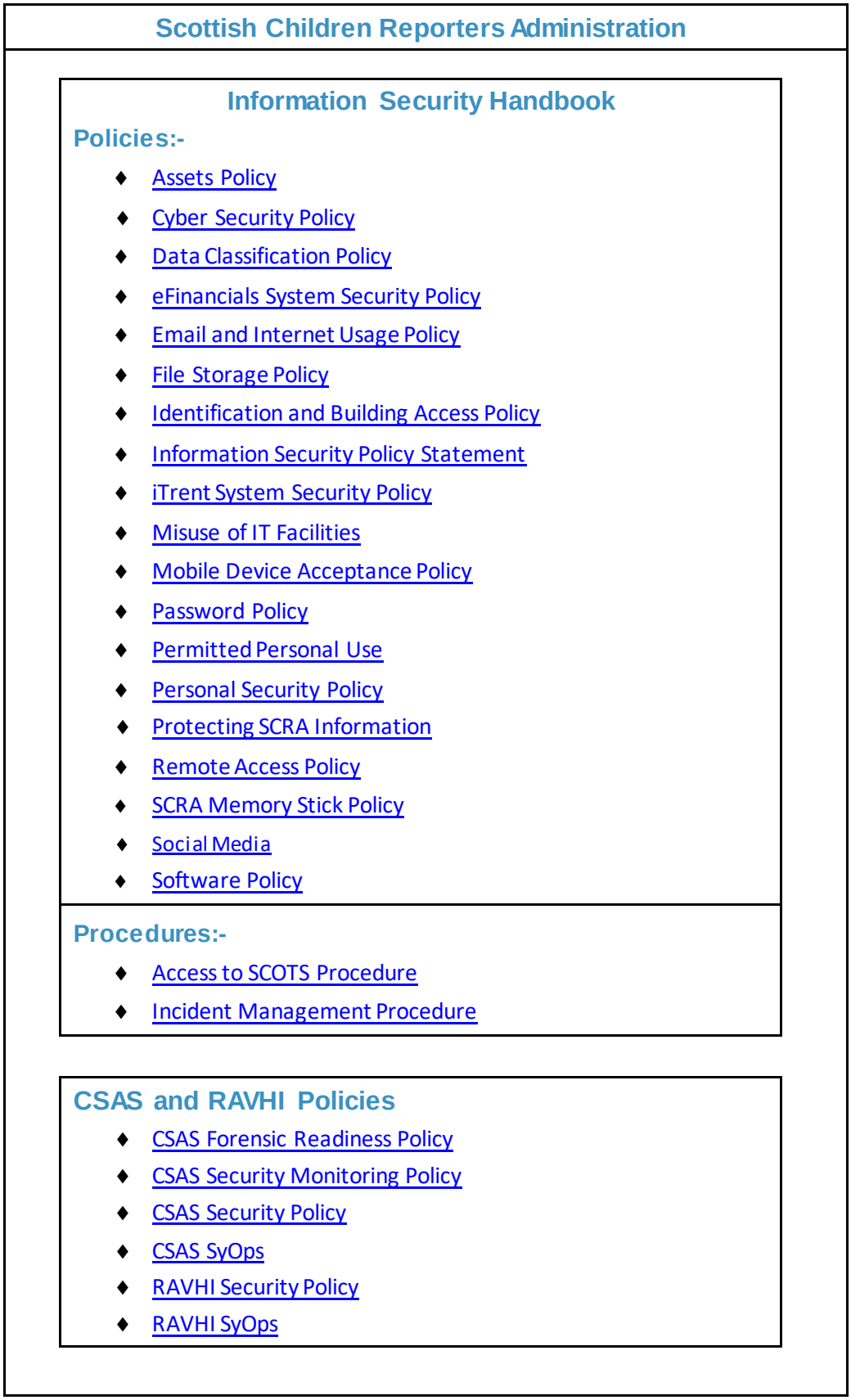


Figure 1 – SCRA policies and procedures on protecting SCRA's data.

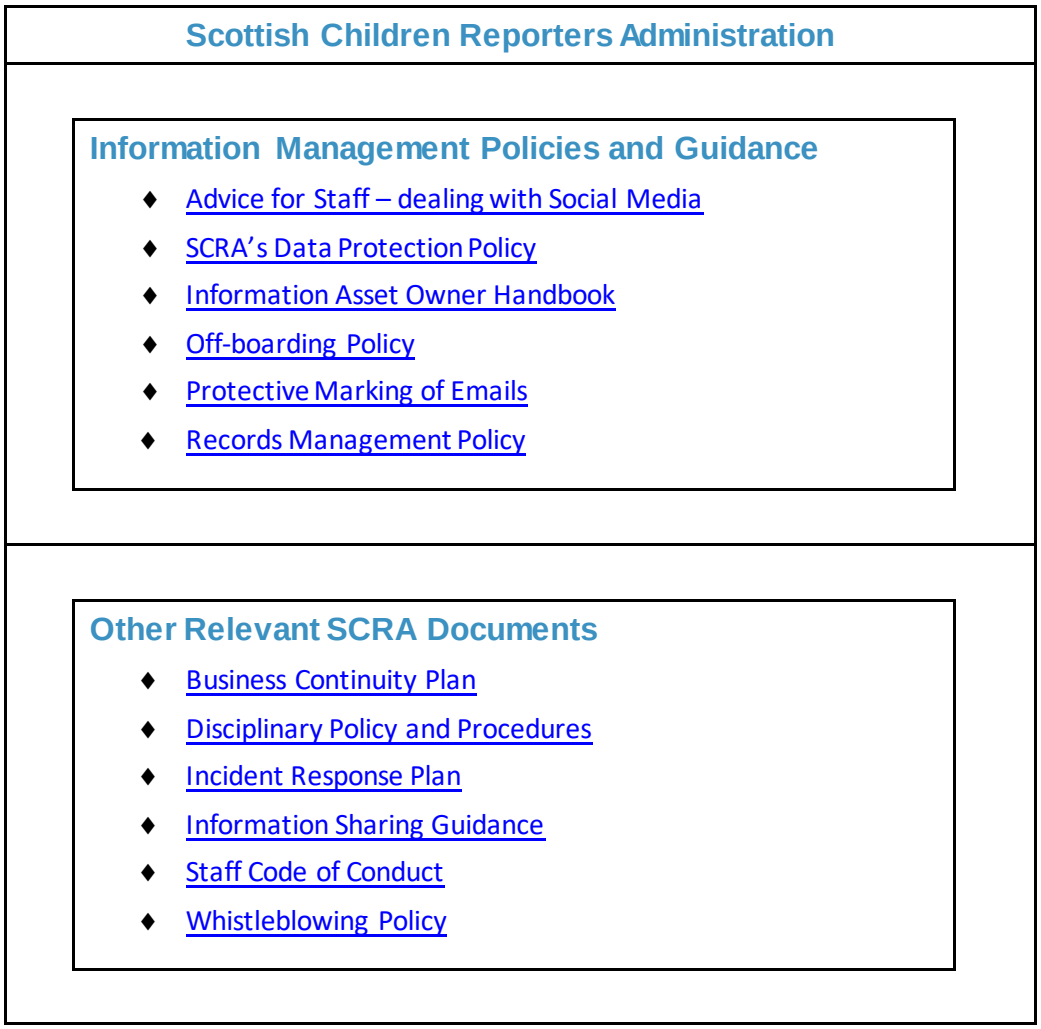


Figure 2 – Other relevant SCRA documents.

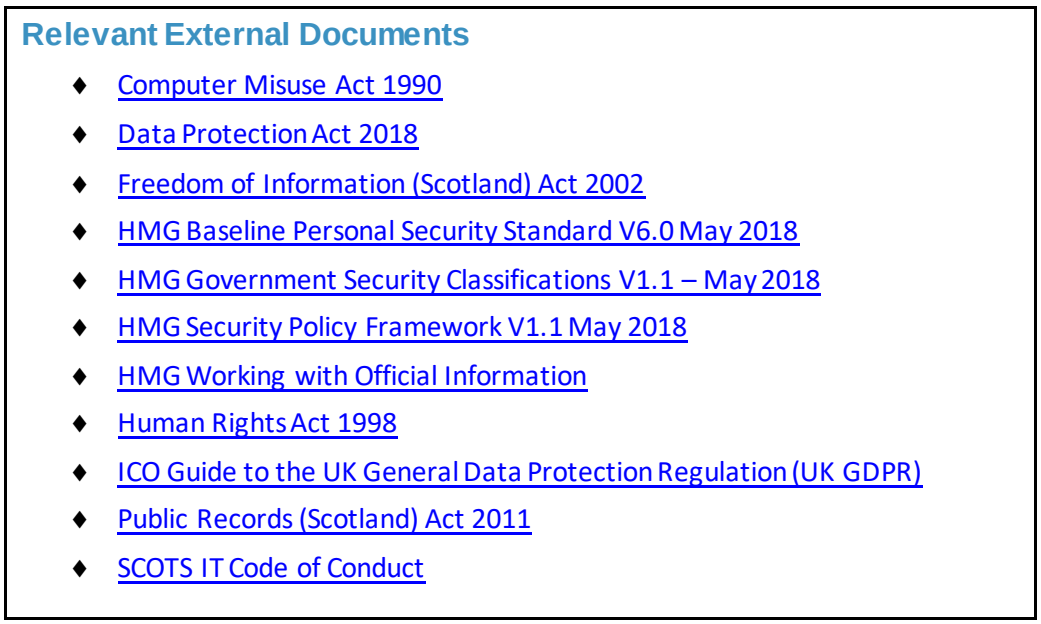
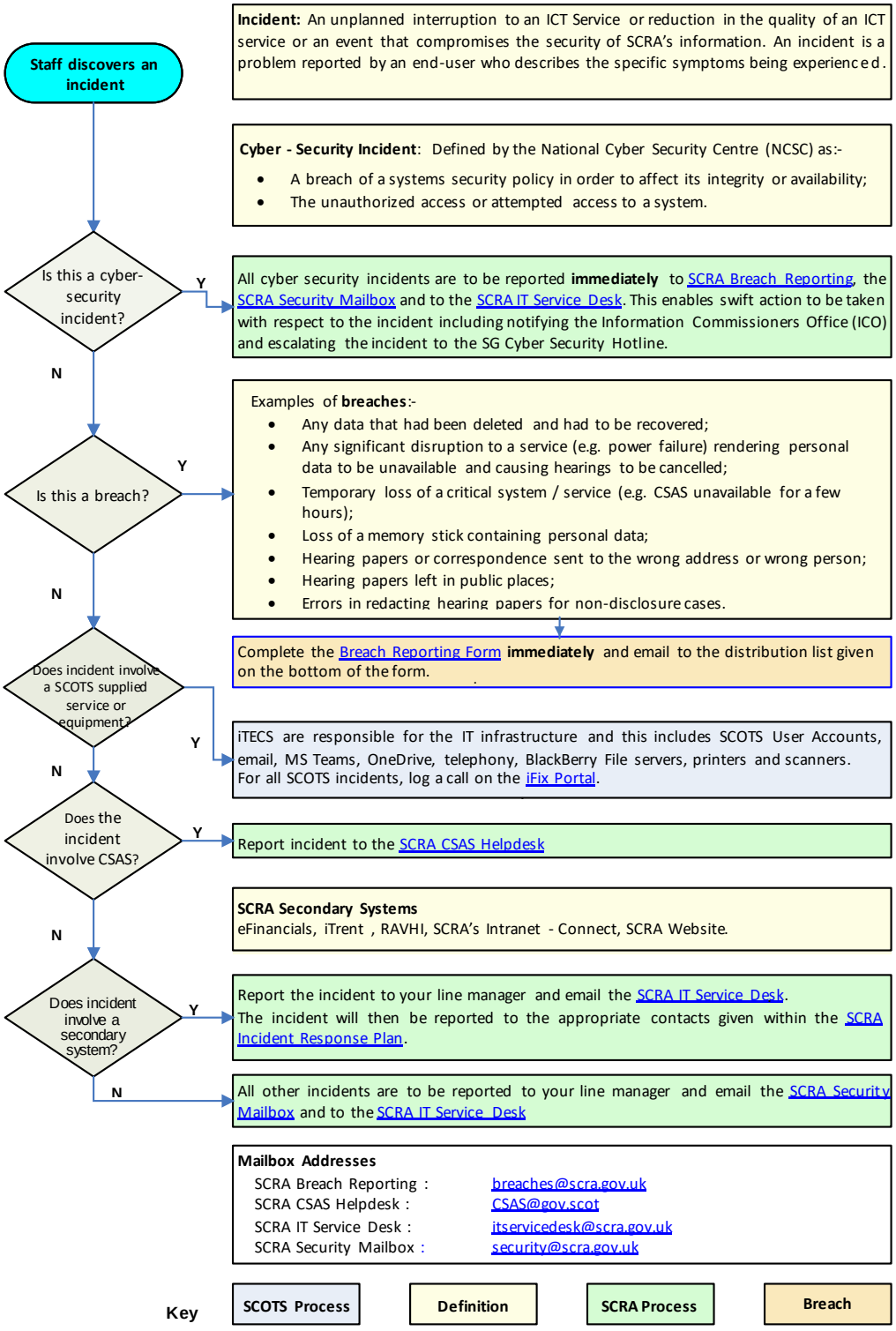


Figure 3 – Specific Government documents that SCRA personnel are expected to comply with - these all have implications on the security of SCRA's data.

Appendix A – Incident Management Flowchart



Note: If the links in the flowchart do not work then the SCRA mailboxes are in SCRA's address list on SCOTS and the link to IFix Portal is published on the home page of Connect.

Appendix B – Information Security Handbook Third Party - Agreement Form

SCRA Information Security Handbook Agreement Form

The Scottish Children's Reporter Administration (SCRA) is actively committed to ensuring the appropriate security, integrity, availability and confidentiality of our own and our clients' information.

Policy

It is our policy to ensure that:

- Information is protected against unauthorised access;
- Confidentiality of information is assured;
- Integrity of information is maintained;
- Regulatory and legislative requirements are met;
- Appropriate business continuity plans are maintained & tested;
- All breaches of information security, actual or suspected, are investigated by competent persons and reported to senior management.

Employee Responsibilities

- To comply with the SCRA's Information Security Handbook and other SCRA policies and documents governing information security.
- To protect any computing resources and information within your area of access or responsibility.
- To discuss additional requirements for protecting computing resources and information with management.
- To report any known or suspected security breaches to management and the Digital Security and Governance Manager.

I acknowledge receipt of SCRA's Information Security Handbook and the SCOTS IT Code of Conduct and that I have read, understood and agree to abide to the terms of these policies. I understand that any infringement of these policies could result in legal action being taken against me or my employer.

Signed:..... Date:.....

Print Name:.....

Please return signed copy to SCRA IT Team, Ochil House, Springkerse Business Park, Stirling FK7 7XE.

Appendix C – Handling of Classified Data

The table below defines the handling arrangements for OFFICIAL classified information and the additional handling arrangements required for OFFICIAL–SENSITIVE classified information.

Activity	Classification : OFFICIAL / OFFICIAL SENSITIVE
MARKING **(of all material, whether paper, electronic, or digital media)**	There is **no requirement to mark** routine OFFICIAL information but **OFFICIAL–SENSITIVE** information should be marked**.** Mark "**OFFICIAL–SENSITIVE** [and the optional 'descriptor' if appropriate]" in capital letters at the top and bottom of each page and in the subject header and body of all emails. **This should be followed by additional handling instructions** detailing distribution and access requirements for this sensitive information.
HANDLING **(of all material, whether paper, electronic, or digital media)**	Consultants, agency workers and SCRA staff have a duty to keep information secure and have a personal responsibility to safeguard any SCRA information that they are entrusted with, or are handing to others. Legacy information or data that uses the old protective markings **does not** require remarking[39].
Email within SCOTS	**OFFICIAL:** No restrictions, however it should be limited on a 'need to know' basis. **OFFICIAL–SENSITIVE:** Permitted on a 'need to know' basis.
Email outside SCOTS	**OFFICIAL:** This information can be sent in the clear over the Internet. For additional protection, encryption should be considered, if appropriate. **OFFICIAL–SENSITIVE:** • E-mail can be sent from SCRA to an e-mail address by email to addresses that are known to belong to a secure domain such as the SCOTS domain (gov.scot), the CJSM domain (cjsm.net) and other approved email domains. • If the email cannot be sent to a secure domain or an approved email domain then other options must be considered – contact the DS&G Manager to discuss the options available.
Moving assets by HAND	**OFFICIAL** Protected at least by one cover/envelope. • Authorisation from the Information Asset Owner if moving a significant volume of assets / records / files. **OFFICIAL—SENSITIVE** as **OFFICIAL** plus carried in a locked bag in order not to draw attention to the contents.

[39] If revising the document then it should be reclassified using GSC and marked accordingly.

Activity	Classification : OFFICIAL / OFFICIAL SENSITIVE
Moving assets by POST/COURIER	**OFFICIAL** Use single, unused envelope. **OFFICIAL—SENSITIVE:** as **OFFICIAL** plus : • Use Tamper proof envelopes for bulky documents e.g. panel papers • Seal the envelope using a SCRA security label. • Never mark the classification on the outside of the envelope. when possible send by secure means such as courier or Special Delivery.
Moving Assets Overseas	Authorisation required from the Information Asset Owner and consult the DS&G Manager to obtain specific handling requirements for moving assets overseas.
Bulk transfer of documents/data	• Requires the approval of the Information Asset Owner. • Assess risks of transferring the assets by conducting a risk assessment. • Seek advice from DS&G Manager for the best course of action to take.
Faxing	Faxes **MUST NOT** be used
MS Teams (as supplied by ITECS)	**OFFICIAL**: Permitted - MS Team Owners are responsible for understanding their responsibilities if allowing external users access to MS Teams. **OFFICIAL–SENSITIVE**: MS Team Owners are responsible for understanding their responsibilities. If using it for communicating OFFICIAL–SENSITIVE information then they must only allow SCOTS users access.
Objective Connect	Permitted for sending **OFFICIAL–SENSITIVE** documents to external contacts.
Photocopying / Scanning	Permitted.
Printing	Staff must use locked print on all SCOTS networked printers that they use.
Physical storage (of documents, digital media, when not in use)	• Protect physically within a secure building by a single lock (e.g. a locked drawer, container or locked filing cabinet). • The Clear Desk Policy should be observed. • Papers should not be left on desks or on top of cabinets overnight.
Electronic storage	• Permitted on SCOTS or on accredited/approved SCRA systems. • Only on SCRA/SCOTS laptops that have their hard drives encrypted. • Any electronic document received marked **OFFICIAL–SENSITIVE** should be saved in SCOTS shared drives in folders with restricted access.
USB Memory Sticks	• Only SCRA approved encrypted memory sticks are to be used. • For temporary storage of **OFFICIAL** and **OFFICIAL–SENSITIVE** data.

Activity	Classification : OFFICIAL / OFFICIAL SENSITIVE
Vscene	An alternative to facilitating virtual hearings (**OFFICIAL–SENSITIVE** data) using RAVHI – see Virtual Hearings Tech Guidance.
Copying to CD or DVDs	Only permitted in exceptional circumstances with prior authorisation from the appropriate Information Asset Owner.
Discussing work on telephones (landline or mobile), in video conferences or in public places	Telephony systems should not be assumed to be secure. **OFFICIAL**: No restrictions. **OFFICIAL–SENSITIVE**: Details of sensitive material should be kept to an absolute minimum.
Disposal and destruction of physical papers	• All **OFFICIAL** and **OFFICIAL–SENSITIVE** data must be disposed of as confidential waste. • Most SCRA offices have confidential waste consoles supplied by SCRA's contracted confidential waste disposal service. • Paper must be shredded or placed within confidential waste consoles or sacks prior to shredding. Confidential waste sacks should not be left unattended.
Disposal of CDs, DVDs	Place disk into an envelope and (with care) break the disk into four pieces. Dispose of pieces in ordinary office waste. Do not recycle.
Disposal of data stored on magnetic or on electronic devices	All magnetic data used to store **OFFICIAL** and **OFFICIAL–SENSITIVE** data e.g. magnetic tapes, hard drives etc. and electronic devices e.g. RAM, USB secure memory sticks, SIMS etc. is to be sent to the SCRA IT Team so that they can arrange for the secure destruction of these devices. Contact the SCRA IT Service Desk if you need more information.