Registers of Scotland

Security and Information Assurance

ICT CODE OF CONDUCT

Registers of Scotland
Departmental Security Group
Policies and Procedures

Department	Security and Information Assurance (SIA)			
Topic	ICT Code of Conduct			
Number	SIA12			
Amended	**By**	SIA	**Date**	11th July 2016

Introduction

1. This Code outlines our policy on the use of Registers of Scotland (RoS) Information and Communications Technology (ICT) facilities.

Scope

2. “ICT facilities” means all forms of computer and communications equipment and software used to create, design, store, transmit, interpret and manipulate information in its various formats. Personal computers, laptops, tablets, printers, telephones, mobile phones, memory sticks, other removable media, televisions, and network technologies are included in this definition.

3. This Code applies to all Users of RoS ICT facilities including third party suppliers, but excludes customers who connect to RoS via our public facing ICT systems.

4. A User is anyone using or accessing, for any purpose, RoS ICT facilities, software and/or data residing on RoS ICT facilities.

Basic Principles

5. Access to RoS ICT facilities, software and the data held on it is restricted to Users authorised by RoS.

6. All Users must act responsibly when using RoS ICT facilities and guard against abuses that disrupt or threaten the viability of RoS ICT facilities.

7. Every User is responsible for the integrity of RoS ICT facilities and must act in accordance with this Code, RoS ICT policies, all relevant statutory provisions, regulations, rules and codes of practice.

8. Users must ensure that they are familiar with the contents of this Code before they use RoS ICT facilities.

Acceptable Use and Behaviour

Do

9. Construct strong passwords and keep them secret.

10. Change passwords regularly, or immediately if you believe someone else knows your password.

11. Use different passwords for all user accounts.

12. Comply with the log out and power off procedures of equipment when leaving the office at the end of the working day.

13. Keep portable equipment (such as laptops, tablets and mobile phones) with you at all times unless these are physically secured.

14. Notify line management immediately if you have system access/privileges to RoS ICT facilities that you no longer require in your current role.

15. Follow the rules and guidance contained in the Annex in the Email Policy E-mail policy

16. Avoid opening up emails with suspicious content and/or from an unknown sender.

17. Take the appropriate level of care with information stored or processed on RoS ICT facilities in line with its business value, sensitivity and protective marking (in terms of the Security Classification policy.)

18. Report information security incidents, threats and weaknesses through appropriate management channels as quickly as possible in line with the Information Security Incident Notification procedures.

19. Report to line management instances where it is suspected that an individual may be misusing RoS ICT facilities.

20. Report through appropriate management channels instances where inappropriate material has been sent or has been inadvertently accessed.

21. Save information in files or emails that contributes to the full understanding of a decision, action being taken, or forms a significant part of the 'story' as a corporate record in line with RoS Documents and Records Management policy.

22. Respect the copyright of all material and software made available by RoS and third parties.

Unacceptable Use and Behaviour

Do Not

23. Disclose your password to anyone else.

24. Write down passwords.

25. Use another individual's user-id and/or password.

26. Attempt to access computer systems or information on computer systems without authorisation.

27. Open up the casings of, remove or re-site computer equipment unless authorised to do so by ICT management.

28. Provide RoS information to third parties without the express authorisation of RoS management.

29. Access and/or pass on information from the registers or other records (e.g. finance/HR/Customer records) for any reason other than a valid business need as part of our assigned tasks and with Information Asset Owner (IAO) authorisation.

30. Distribute sensitive or valuable information without authority.

31. Email sensitive material over the Internet unless the email is appropriately protected in line with guidance in the Safeguarding RoS Information guide.

32. Download, distribute, store or display images or text which could be considered offensive, e.g. material of a sexual, pornographic, paedophilic, sexist, racist, religious, libellous, threatening, defamatory, of a terrorist nature or likely to bring RoS into disrepute.

33. Forge email signatures and/or headers, generate and/or distribute 'chain' or 'junk' email.

34. Play computer games on RoS ICT facilities.

35. Use RoS ICT facilities for gambling purposes.

36. Purchase software directly on behalf of RoS unless authorised by ICT management.

37. Install any software (e.g. shareware, freeware, public domain, personally acquired, evaluation software) on RoS equipment unless expressly authorised to do so by ICT management.

38. Use, download, copy, store or supply copyright materials including software and retrieved data, without the permission of the copyright holder or under the terms of any licence held by RoS.

39. Modify, de-install, copy or delete software on RoS equipment unless expressly authorised to do so by ICT management.

40. Terminate/disable protective software such as anti-virus software on RoS equipment.

41. Connect any unauthorised devices, including privately owned devices, to RoS equipment or the RoS network. RoS ICT facilities must not be used for a power source.

42. Copy RoS information to privately-owned equipment or portable media such as DVDs and memory sticks unless authorised to do so by the appropriate Information Asset Owner as detailed in RoS Information Asset Register.

43. Delete, alter or otherwise interfere with the RoS email disclaimer when using the corporate email system.

44. Make improper use of RoS official templates.

45. Possess, distribute, reproduce or use computer programs for reasons such as scanning networks, intercepting information or password capture unless specific authority is obtained or held from the Security and Information assurance (SIA) team / Business ICT team.

46. Distribute private or personal information about other people without management authorisation.

47. Provide your corporate email address to email mailing lists for purposes other than those that are RoS business-related.

48. Use RoS ICT facilities for private commercial activity, political activity or private use of chat rooms.

49. Disseminate or print copyright materials in violation of copyright laws.

Personal Use

50. You are permitted to make limited personal use of RoS ICT facilities in your own time, either when clocked out for staff on Flexible Working Hours (FWH) or outside

normal working hours for those not on FWH, or on a recognised break. This use must not disrupt the conduct of RoS business operation or other RoS business users.

51. The Keeper's registration as a data controller under the Data Protection Act 1998 only covers information held on the RoS computer systems for RoS work-related purposes. Any personal or non RoS work related documents containing details of living persons should only be stored temporarily while they are being prepared, and must then be deleted from RoS ICT facilities.

52. The Civil Service Code of Conduct forbids use of RoS ICT facilities or the Internet to prepare or research material in connection with running a private business or any other material that could be held to be of direct financial benefit to the user or any third party connected to them.

53. You are allowed to send brief personal emails using the corporate email system but the message sensitivity option in Outlook should be used to mark such emails as 'personal'. You should discourage large incoming personal emails, as these can have an adverse performance impact on the corporate email system and prevent work-related emails being delivered promptly.

54. You must comply with RoS social networking guidelines.

55. If you are studying for any form of academic or professional qualification, with RoS support, you may use RoS ICT facilities to prepare study material with line manager approval.

56. RoS accepts no liability for any loss or damages suffered by any individual as a result of personal use.

Monitoring

57. The SIA team is responsible for periodically conducting audits to confirm that information in home fileshare and email folders are not in contravention of this Code.

58. RoS conducts random audits of RoS computers, including portable equipment to ensure that RoS is complying with all software licences.

59. All corporate email activity including traffic into or out of RoS is logged and a record is kept of every Internet site accessed whether the attempt was successful or not. This record shows the originator's user name, date, time and full site address of attempted access, whether successful or not.

60. As part of standard monitoring procedures baseline information in the usage logs will be regularly examined. Any evidence of misuse will be investigated.

61. Any email may be viewed at any time as part of this monitoring process, and therefore cannot be regarded as private. RoS may access email messages relevant to the business in staff corporate email boxes whilst the member of staff is absent from work, for example on leave.

62. Line managers will be alerted and disciplinary action considered if there is cause for concern about inappropriate use or excessive use in accordance with this Code. It will be for senior managers to determine what is deemed excessive use within their business function.

63. RoS will investigate instances where inappropriate information about the RoS business operation or their staff is posted on social networking sites. If the source of the inappropriate information is RoS staff, then disciplinary action will be considered.

Compliance

64. We are all required to familiarise ourselves and fully comply with this Code of Conduct and ignorance of the code will not be accepted as a defence at a disciplinary hearing.

Misuse and Disciplinary Process

65. Anyone who misuses RoS ICT Facilities may be committing a criminal offence.

66. The list of unacceptable uses and behaviours narrated in this Code of Conduct is not exhaustive. Instances of misuse will be treated as misconduct liable to disciplinary action. Serious offences may be considered gross misconduct and could lead to dismissal, even for a first offence.

67. Any possible cases of misuse will be drawn to the attention of the line manager who will decide what action to take after consultation with HR. Attempts to access, active accessing, downloading and transmission of pornographic, racist, sectarian and offensive material will always be treated as gross misconduct. In extreme cases it may be necessary to involve the police, if there is prima facie evidence that a criminal offence has been committed.

Contact details

68. For further guidance on this Code, contact the SIA team ext. 3333 or email IT.SecurityOfficer@ros.gov.uk