COMPUTER USE POLICY

Policy Number: 32

Document Control

Owner	Reviewers	Approver
Technology and Security Architect	Head of People & Performance Head of Internal Audit Technology Manager	Head of People & Performance Head of Internal Audit Head of I&C

Version	Date Issued	Status	Description	Review Date
Finalv1.0	8th May 2018	Final	Reworked to support GDPR initiative	Apr 2019

Purpose

The purpose of the **Computer Use Policy** is to ensure a clear understanding of acceptable use of Scotmid's Computing Resources by any and all of Scotmid's employees, contractors, consultants or service partners who access Scotmid's Computing Resources.

If you have questions on this policy, employees should refer to their Staff Handbook or contact Innovation & Change. Non-employees should raise questions with the Head of Department of the Scotmid area procuring their service or with Innovation & Change directly.

If you are concerned your Scotmid UserId, password or any of Scotmid's Computer Resource has been compromised please contact Innovation & Change immediately on 0131 335 4567.

Context

Scotmid recognises using computer equipment and systems is an integral part of everyday work, providing Users with a capability to access the Society's information and complete business tasks as part of fulfilling their roles.

Scotmid's Computing Resources and the confidentiality, integrity and availability of the information they contain are central to the effective operation of Scotmid's business. The access and security of Scotmid's Computing Resources and data must therefore be controlled, in line with best practice, to prevent accidental or malicious breach, interruption, destruction or loss of Scotmid's Computing Resources or data.

Scotmid uses the Information Commissioners Office and the UK Government's recommended Cyber Essentials and 10 Steps standards for guidance on appropriate controls and policy for its Computing Resources and so this Computer Use Policy.

Key Definitions

- **"Scotmid"** refers to the Scottish Midland Co-operative Society Limited and all of its subsidiary and associated companies and undertakings.
- **"Computing Resources"** includes, but is not limited to the following: computers, servers, storage and back-up infrastructure, laptops, mobile phones, tablets, handheld terminals, tills, printers, PIN entry devices, scanners, all software and internal or external data and voice communications networks, wifi and network equipment and wiring.
- **"Innovation & Change"** (also known as **"I&C"**) is the Scotmid department that supports and maintains Scotmid's Computing Resources.
- **"Malware"** short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, ransomware, spyware and other malicious programs specifically designed to gain unauthorized access to a computer system.
- **"Portable Computer Equipment"** mean handheld computer and electronic equipment, including but not limited to: laptops, mobile phones, tablets, hand held terminals (HHTs), portable printers, scanners, projectors etc.
- **"Portable Media"** means readily transportable items used to store data electronically which can be attached to computer equipment for data transfer, including, but not limited to: detachable external disk drives, media players, USB sticks, flash memory cards, CDs, DVDs, Dictaphones etc.
- **"Users"** refers to any full/part time staff, or contractor and other persons or entities granted access to Scotmid Computing Resources and Services.
- **"UserId"** refers to a User's login name entered when accessing a system.

Scope

The policy applies to all Users of Scotmid's Computing Resources regardless of geographical location or connection method or device. This includes all employees, full or part-time, on permanent, interim, fixed term or temporary contracts of employment.

The policy also applies to any non-employees who have been granted by Scotmid, access to Scotmid's Computing Resources. The Head of the Department for the department granting access to non-Scotmid Users must ensure that such Users are made fully aware of and agree to comply with this policy.

Policy

Access & Passwords

1. Access to Scotmid's Computer Resources is controlled by the use of UserId's and associated passwords. Users are responsible for safeguarding their passwords. Individual passwords should not be written, printed, stored on-line or given to others. Users must not use the same password for accessing Scotmid Computer Resources and non-Scotmid systems (e.g. personal email accounts).
2. All Computer Resources, where possible, should be proactively locked by the User if they are leaving the equipment unattended – even for a short period of time.
3. Users are responsible for all actions taken by their UserId and must not share their UserIds and passwords with others.
4. Users must not access, or attempt to access, any Computer Resources by using someone else's UserId and password.
5. Users must not access, or attempt to access, specific transactions, functions or files of any Computer Resources where they do not have the relevant authority. The ability to access does not imply a right to such access.

Computers, Peripherals & Media

6. All Computer Resources purchased by Scotmid remains the property of Scotmid and must be returned to Scotmid upon request or before the User's last working day for Scotmid.
7. Downloading and installing of software or altering any Computer Resources is prohibited without first receiving express authorisation to do so in writing from I&C.
8. If a User thinks they have a virus or if they are unsure about virus protection then it is important that they seek assistance from I&C immediately.
9. Users must not attempt to attach or install additional hardware or peripherals (e.g. CD-ROM or external drive devices, cameras etc.) to Scotmid's Computer Resources without prior permission from I&C.
10. All mobile phones, tablets or other Portable Computer Equipment are prohibited from being plugged into Scotmid's computer USB ports for charging or data transfer. Separate dedicated 3-pin plug chargers must be used for charging.
11. Unless a regular data transfer procedure with an external source has been agreed with I&C, all Portable Media or data transfers into the Society from external companies must be presented to I&C for scanning and validation prior to being connected to Scotmid's Computing Resources.
12. No User data is to be stored directly on (i.e. the 'c: drive') any Scotmid computers. Such data is not backed up and will be lost in the event of a computer failure. Local data stored on mobile phones and tablets is not backed up by Scotmid and the User is responsible for taking any necessary back-up copies required to mitigate the loss of data in the event the device is lost, broken or fails.
13. Scotmid Laptops must connect directly to the Society network every 30 days for at least 2 hours via branch Wi-Fi or wired connection to allow security updates to be received and installed.

14. Users must exercise reasonable care when using, transporting or storing Portable Computer Equipment and Portable Media to prevent loss, damage or theft and on no account leave the equipment unattended in a public place or on display in a parked vehicle.
15. Portable Media must be locked away when not in use. Portable Computer Equipment, if not taken home, must be locked away in a drawer or cabinet overnight and not left on its docking station.
16. The acceptable use of Society provided and **"Bring Your Own Device (BYOD)"** smart devices –phones and tablets - is further set out in the **Mobile Phone Policy**.

Messaging and Internet Access

17. Users should communicate via email, instant messaging, voice/web/video conferencing mediums in a professional manner. All such communications are subject to Scotmid's policies.
18. Fraudulent, defamatory, abusive, harassing, menacing, indecent, obscene or any other unlawful material may not be accessed, viewed, created, stored, processed, displayed, sent or posted from Scotmid's Computer Resources.
19. Scotmid is conscious that Users may from time to time receive external messages (email, SMS or instant messages) or return web search results which potentially breach our policies e.g. of a pornographic or sexually explicit nature. Such messages when received should be deleted immediately and not forwarded or shown to other Users. Any inappropriate web pages accessed accidentally should be closed immediately. If you are concerned you have accidentally breached a Scotmid policy you should notify your line manager as to the nature of the event and breach as soon as you can.
20. Scotmid uses a web site classification system across the Internet to assist in navigation of sites and to help prevent accidental access to unsuitable or risky sites. Scotmid restricts access to only certain categories of site. However this does not imply that any site, which the User can access, is an acceptable site for business purposes.
21. Users must be aware of and consider the risk when accessing messages of fake 'phishing' messages (email, SMS, instant messages) with Malware infected attachments or website download links.
22. Users must be aware and consider the risk, when browsing the internet, of possible fake websites or hacked public websites which may be used to capture valuable User information (e.g. password, date of birth etc.) for cyber crime purposes.

Personal Use

23. The Society's Computer Resources, including internet access, all messaging applications and systems (email, SMS, instant messaging, video/web/voice conferencing), computers, phones, mobile phones and tablets are provided for Scotmid's business purposes.
24. Branch Computer Resources are not individually assigned and are not for personal use. The only exception is Branch 'guest' wifi which employees can use outside of shifts or on breaks.
25. A reasonable amount of personal use of PCs, laptops, tablets, mobile phones, messaging applications and internet access is permitted for Head Office and Field employees - although it must not interfere with the User's work or that of other Users.
26. Users must not play internet based computer games or stream/download personal music, videos or other media on Scotmid's Computer Resources.
27. Users are prohibited from using Scotmid's Computing Resources for any other (non-Society) commercial purposes, nor for the transmission of personal advertisements, solicitations, promotions, destructive programs, political material or any purposes that may bring Scotmid into disrepute.
28. Fraudulent, defamatory, abusive, harassing, menacing, indecent, obscene or any other unlawful material may not be accessed, viewed, created, stored, processed, displayed, sent or posted from Scotmid's Computer Resources.
29. Outside of work, Users should be aware of and adhere to Scotmid's **Social Networking Policy.**

Data

30. Scotmid has a legal obligation under UK data protection legislation to ensure that the Personal Information of any individuals it holds (e.g. employees, customers, members etc.) is held securely and processed fairly and lawfully. Users have a legal responsibility to assist Scotmid to comply with its data protection obligations. Users must read and adhere to the **Employee Data Responsibility Policy**.

31. Users must comply with all software licenses, copyrights and intellectual property rights. Users must not make copies of software, copyrighted media or data unless specifically authorised to do so.

Joiners, Movers and Leavers

32. It is the responsibility of the Line Manager to complete and authorise a 'New user Request' or 'Request Change to Existing User' form at least 5 working days prior to any User joining, moving or leaving the Society to notify I&C to assign, change or revoke the Users Computer Resources access. Managers should also obtain any passwords encrypted files created by the User prior to their departure.

Monitoring

33. To ensure the on-going confidentiality, integrity and availability of the Society's Computer Resources and data, Scotmid deploys and has in constant operation security and logging tools. Examples includes antivirus software, computer/network/wifi firewalls and monitoring, email spam filtering and attachment scanning, file monitoring, web filtering and monitoring, mobile device management software and application transaction logging. As part of this, User emails, web site, landline and mobile phone usage is logged and is available to be reviewed if a breach of policy is suspected.

34. Breach of this or related Policies will be taken seriously and, depending on the severity of the matter, may lead to disciplinary action including termination of employment.

If you are concerned your Scotmid UserId, password or any of Scotmid's Computer Resource has been compromised please contact I&C immediately on 0131 335 4567.

If you believe you may have inadvertently breached this or related policies by accident, please notify and discuss with your line manager as soon as possible.

Law

35. Users must comply and be aware the use of Scotmid's Computing Resources falls under current applicable UK and Scots law, including but not restricted to:
    a) Intellectual Property law including laws concerning copyright, trademarks and patents.
    b) The Computer Misuse Act 1990
    c) The Data Protection Act 1998 and General Data Protection Regulation 2018
    d) Interception and monitoring laws of the Regulation of Investigatory Powers Act 2000
    e) Terrorism Act 2000, the Terrorism Act 2006 and the Counter Terrorism and Security Act 2015

36. This policy is revised periodically, as the need arises, and updates published on Scotmid's intranet.

Related Policies and Documents:

This policy should be read in conjunction with the following other Scotmid policies and documents:

a) Staff Handbook
b) Employee Data Responsibility Policy
c) Mobile Device Policy
d) Social Networking Policy

DECLARATION
I confirm that I have received a copy of this policy and that I have read and understood it.

Name: _____

Signature: _____ Date: _____