Information Acceptable Use Policy

Version:	3.6	Status:	Approved
Author/Owner:	Digital Services Manager	Approval/Review:	KITGG
Approval Date:	4 April 2019	Next Review Date:	30 April 2020

Introduction

1. Our information is a vital asset and must be protected by appropriate measures to ensure information systems integrity and security.
2. Employees must always act with integrity and follow our Code of Conduct.
3. This policy specifically describes what is expected of colleagues when they manage information.

Scope

4. This policy is mandatory for all employees, contractors and consultants employed by Audit Scotland. Failure to comply with this policy may result in disciplinary action.
5. This policy encompasses all Audit Scotland digital systems and devices that store, process or transmit information.

Information Classification

6. Audit Scotland uses three information classifications:
    - 6.1. Public – Information which has been published or would be readily released under a Freedom of Information (FOI) request.
    - 6.2. Controlled – Information that has not been published and would require review before sharing with others.
    - 6.3. Personal – Personal data as defined by the Data Protection Act (DPA) and General Data Protection Regulation (GDPR), which will never be shared except under the specific provisions of the DPA and GDPR.

Devices

7. Audit Scotland devices must always be kept secure;
    - 7.1. Our devices must not be given, loaned or used by anyone not employed by Audit Scotland.
    - 7.2. Access must not be provided to unsecured on attended devices, unless employed by Audit Scotland.

7.3. Devices must be stored securely, wherever possible locked away and out of sight.

7.4. Any device or media no longer in use or which needs to be destroyed, must be returned to Digital Services for secure disposal as per the **IT Disposal Policy**.

7.5. As specified in the Clear desk and screen policy, when not in use, systems must be locked with a password/PIN to prevent people from viewing information on the screen.

8. Employees must take appropriate care of Audit Scotland devices and wherever possible protect it from physical damage.

9. Employees must only connect Audit Scotland devices to authorised networks. ①

9.1. Laptops and Citrix thin clients must not be connected to any other network via Ethernet cable, other than an Audit Scotland network.

9.2. Mobile devices and laptops may be connected to Audit Scotland services via secure third-party Wi-Fi or data services provided by Audit Scotland.

10. Transfer and/or storage of information must only occur using the appropriate level of security and encryption. ②

10.1. Personal and controlled information must only be transferred and/or stored on Audit Scotland encrypted systems, networks or devices. The Digital Services team can assist colleagues in selecting an appropriate system or device. ②

10.2. Public information may be transferred and/or stored on systems, networks or devices. If unsure about the classification of the information, always use Audit Scotland encrypted systems, networks or devices.

11. Audit Scotland mobile phones must comply with the Remote working policy and are only to be used for appropriate business activities.

11.1. Audit Scotland phones must not be used for premium rate services.

11.2. Audit Scotland phones must not be used for international calls without express written permission from an Assistant Director or Director.

11.3. Audit Scotland mobile phone data usage is monitored and must not be used for excessive personal use that exceeds the allocated data cap or allocated call minutes. Wherever possible WiFi should be used. ③

11.4. Audit Scotland mobile phones voice call usage is logged. ③

11.5. All employees are responsible for adhering to the law in respect of not using a mobile phone while driving a vehicle. ④

12. Audit Scotland permits the use of personal devices to access Audit Scotland's services as specified in the Working with personal devices policy.

13. Internet of Things (IoT) devices must not be connected to the Audit Scotland network or WiFi without specific written authorisation from a member of the Digital Services Management Team (DSMT).

14. Audit Scotland devices and systems must only be used for work appropriate activities. ①

    14.1. Personal (non-work related) files must not be stored on Audit Scotland devices and systems.

    14.2. Information and media that are inappropriate and/or illegal must not be stored or viewed on Audit Scotland device. ① ⑦ ⑧ ⑨

15. Employees must return all Audit Scotland devices to a member of Digital Services or their line manager before leaving the organisation.

16. If an employee is unable to locate an Audit Scotland device or it is stolen, they must immediately report it to a member of the Digital Services team, Corporate Governance Manager, their line manager and the appropriate Information Asset Owner. ②

Software and services

17. All software and software licences purchased by Audit Scotland are the sole property of Audit Scotland. They may not be transferred, loaned or sold without the explicit permission of a member of the DSMT ⑦

18. All purchases of new or additional software that handle personal information must be approved by a member of the DSMT.

    18.1. Agreement to the User Licencing Agreement (ULA) or licence terms can only be made by a member of the DSMT. ⑦

    18.2. Employees must not install or remove software from Audit Scotland Secure Zone devices. Only members of the Digital Services team may install or remove software from Secure Zone devices. ①

19. All internet services that store or process Audit Scotland information must be reviewed for privacy impact and **pre-approved** by a member of the DSMT and the Corporate Governance Manager.

20. Changes to the security, configuration or function of Audit Scotland devices, software or services must only be made by a member of the Digital Services team. ①

    20.1. Employees must not make any attempt to bypass, disable or change any security, configuration or function of Audit Scotland device, software or services. ①

    20.2. Employees must immediately report any suspected hacking (attempt to bypass, disable or change any security, configuration or function) to a member of the Digital Services team ①②③

21. Access to Audit Scotland's devices, software and services is regulated by the Digital access control policy.

    21.1. Passwords must comply with the **Password and Connection Standard,** be:

        21.1.1. a minimum of 12 characters and include special, mixed case and numeric characters,

        21.1.2. kept safe and confidential, and

        21.1.3. combine with additional Multi Factor Authentication (MFA) when outside Audit Scotland offices.

22. All Audit Scotland devices, software and services must be appropriately protected from malware, hacking and ransomware. ①②⑨

    22.1. All Audit Scotland laptops must be connected to the Audit Scotland network every 30 days for updated security patches and anti-malware signatures.

    22.2. All Audit Scotland mobile devices must be configured to receive regular system patches and app updates and where required, staff must apply security patches as soon as possible.

    22.3. Employees must take appropriate care with email and instant messaging, alerting a member of the Digital Services team if they have any concerns about **any** suspicious activity or content. ①②③

    22.4. Employees must take appropriate care accessing and downloading content from the internet. They must not download material that appears suspicious or from an unknown site and must contact a member of the Digital Services team if they have any concerns. ① ⑦ ⑧ ⑨

    22.5. Employees must immediately alert a member of the Digital Services team if their system is showing unusual dialog boxes or behaving in an unusual manner.

23. Audit Scotland provides email, internet access, instant messaging, together with voice and video conferencing for Audit Scotland work related purposes.

24. Audit Scotland logs and scans all email, internet access and instant messaging for malware and may block inappropriate or dangerous content. Audit Scotland also logs the duration and destination of all voice and video conferencing.

25. Employees who need to access social media during their work must follow guidance in the Social Media Handbook.

    25.1. Employees are strongly encouraged to use their own devices for personal internet use. Audit Scotland devices can be used for limited personal internet access.

    25.2. As specified in the Encryption policy, personal information must never be sent send via email or uploaded to an external website without a suitable level of encryption. ②⑨

25.3. Employees must only use Audit Scotland email, social media, instant messaging, voice and video conferencing for work purposes. ⑧

25.4. Employees must never use personal email, social media, instant messaging, voice and video conferencing to present personal opinions that may be misconstrued as Audit Scotland's opinions.

26. Employees who are required to use client or third-party computer devices must familiarise themselves with the client's own information security policy and accept the terms of that policy. ①

26.1. Employees must never reuse passwords used for Audit Scotland systems on client or third-party computer device.

Monitoring and Breach of Policy

27. Any member of the DSMT has the right to suspend all Audit Scotland system access to any person suspected of breaching this policy, pending investigation.

27.1. An employee who suspects a breach of this policy, must report it immediately to a member of the Digital Services team and their line Manager, or if the matter us particularly sensitive a senior member of the Human Resources team.

28. Monitoring of all systems takes place to manage security risks, ensure appropriate use, track costs and meet our governance requirements.

28.1. Monitoring must not contravene our obligations under relevant legislation. ③⑥

28.2. Monitoring must be proportionate, justified, controlled, not unnecessarily intrusive and adhere with GDPR best practice guidance. ④⑨

29. Any serious breach of this policy may be considered gross misconduct.

30. Serious misuse of the computer system is a criminal offence under The Computer Misuse Act (1990) and other relevant legislation. Any activity amounting to criminal conduct will be reported to the police.

Relevant legislation

31. Any use of Audit Scotland devices and services must comply with the appropriate legislative regulations. Sections of this policy directly related to legislation are marked as below:

① The Computer Misuse Act (1990)

② The Data Protection Act 1998 (DPA until 25 May 2018 then GDPR)

③ Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

④ Road Vehicles (Construction and Use) (Amendment) (No. 4) Regulations 2003

⑤ The Freedom of Information (Scotland) Act 2002

⑥ Regulation of Investigatory Powers (Scotland) Act 2000

⑦ Copyright, Designs and Patents Act 1988

⑧ Communications Act 2003

⑨ Civic Government (Scotland) Act 1982 & Audio visual Media Services Regulations 2014

⑩ General Data Protection Regulation.

Change Log

Version	Date	Author	Description
2.0	29/08/2013	IT Manager	Renamed from acceptable use policy, re-structured and updated, approved by board 29/08/2013
2.1	06/03/2014	IT Manager	Updates to reflect changes in technology and legal environment
2.1.1	30/08/2015	IT Manager	Minor updates to include clear desk and clear screen policy. Amendments reviewed by KITGG August 2015 and Management Team September 2015
2.2	31/03/2016	IT Manager	Title changed to Acceptable Use Policy. Major review and revision. Numerous updates to reflect technical, organisational and legal changes. Text refined to be more concise and specific. Sections removed to separate policies.
3.0	05/04/2016	IT Manager	Major review and changes made by KITGG. Text revised and expanded to be more specific. Name changed from Acceptable Use Policy to Information Acceptable Use Policy. Approved by KITGG.
3.1	07/06/2016	IT Manager	New section of Relevant legislation listing acts and cross-referencing policy sections
3.1	09/06/2016	IT Manager	Amendments reviewed and approved by ISMT. For KITGG approval at next meeting.
3.1	23/06/16	IT Manager	Approved by KITGG.
3.2	25/07/16	IT Manager	Statement added to 5.4 on secure disposal of media and devices. Approved by ISMT and issued for KITGG approval.
3.2	27/07/16	IT Manager	Approved by KITGG.
3.3	23/08/16	IT Manager	Minor correction to password length.

3.3	12/05/17	Digital Services Manager	Additional statement added in 23.1, reference made to Data Protection regulation changes in 2018, Information Services changed to Digital Services. Policy approved by KITGG.
3.4	12/11/17	Digital Services Manager	New sections to cover procurement of web services that store or process Audit Scotland information and network attachment of IOT devices. Approved by KITGG.
3.5	23/04/18	Digital Services Manager	Policy reviewed and approved by KITGG as part of annual refresh process. Minor updates made, including references added for GDPR.
3.6	04/04/19	Digital Services Manager	Annual effectiveness policy review. Minor policy changes and updates to links. Policy approved by KITGG.