WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Document reference:	Version 3.0
Date issued:	April 2015
Contact:	Matthew Jubb

Information Security Policy

Revision History

Version	Summary of changes	Date
V1.0	First version finalised.	February 2006
V1.1	Change of Information Security Officer, amended para 29 such that connection to home broadband network is permitted	October 2007
V2.0	Major revision including more detailed guidance on “care of equipment” and “obtaining business data from audited bodies”.	October 2008
V2.1	Change reflecting that WAO equipment e.g. laptops, memory sticks can be left unattended in vehicles for up to 4 hours if hidden and locked in the boot, or equivalent	May 2009
V2.2	Revision to section on Security Monitoring and Enforcement, explaining that routine monitoring will take place. The monitoring will check staff compliance with the law and this Information Security Policy. Access to social networking and external email websites prohibited.	July 2010
V2.3	Inclusion of material to provide clarification of unacceptable use of information processing facilities. Inclusion of new appendix 3 setting out detailed routine monitoring policy.	September 2011
V3.0	Major revision – Information Security Policy now focuses on practical requirements. Higher level information processing principles, together with roles and responsibilities, are now found in the separate Information Governance Policy.	April 2015

Table of Contents

Summary

1. The requirements in this policy apply to all employees, non-executive members and contractors, whether employed via an agency, or directly. For brevity, in this document, “staff” is defined to mean all of these categories of people.

2. This policy describes the practical steps staff must take in order to keep the organisation’s information secure.

3. Whereas this policy has a practical focus, it should be read in conjunction with the Information Governance Policy, a higher level document which covers the principles of information processing and the related roles and responsibilities.

4. All staff are required to make themselves familiar with this Information Security Policy, and to confirm that they have read and understood the contents.

5. This document contains the official policy of the organisation. The revision history is shown on the cover sheet.

Information Security Management System

6. WAO has adopted the International Standard for Information Management Security Systems (ISO 27001) whose principles include:

a. systematically examining and assessing the WAO’s information security risks, taking account of the threats, vulnerabilities, and impacts;

b. designing and implementing a coherent and comprehensive suite of information security controls and/or other forms of risk treatment to ensure risks are reduced to an acceptable level; and

c. adopting an overarching management process to ensure that the information security controls continue to meet the organisation’s information security needs on an ongoing basis.

Staff Responsibilities

Usernames and passwords

7. Each staff member will be provided with a username-password combination for use with WAO systems, for example, when logging on to a laptop, or retrieving a monthly payslip. Such passwords must not be shared with colleagues. Please contact the IT team if you are not able to get access to the systems or resources you need.

8. Passwords should be set to something memorable, and never written down.

Connecting personal or non-WAO equipment

9. Personal or visitors' smartphones or computers may be connected to the Internet via WAO's guest WiFi – search for 'guest WiFi' on the Hub for details. Non-WAO equipment must not be connected in any other way – for example via a network cable.

Care of equipment

10. Although data on WAO laptops and smartphones are protected by encryption, staff must take reasonable care of WAO equipment. Theft or loss of equipment due to a failure to take reasonable care will be treated as a serious matter.

11. Staff must not leave WAO equipment unattended where it is at risk of theft – for example, open (i.e. screen unlocked) on the table on a train journey, or in an unlocked hotel meeting room during lunch.

12. WAO equipment can be left unattended in a car for up to 4 hours, provided it is hidden from view and the car locked – but never overnight.

13. Staff may leave WAO equipment unattended at office sites where there is reasonable "perimeter security" i.e. measures to prevent unauthorised people from getting into the office, or at home.

14. All equipment must be returned via the line manager when employment finishes.

Obtaining and Communicating Information

15. WAO classifies information into three categories. Different handling precautions apply, depending on the category:

a. **Very sensitive data—**this will usually include significant personal data, for example, an audited body's payroll file containing names, addresses and bank details used with computer-aided audit techniques (CAATs), or information submitted by WAO to the Department for Work and Pensions containing details of employee pension contributions. Such information should only be transferred and processed:

   i. following prior arrangement with both the WAO's single point of contact (SPOC) and the audited body's SPOC, and

   ii. by a secure encrypted method, such as web-based encryption or hand to hand between pre-arranged named contacts by encrypted memory stick;

   iii. in accordance with specific procedures authorised for the business process in question. For example, CAATs data are subject to a specific policy, may only be stored on a standalone, encrypted machine which does not leave the WAO office, and must be deleted as soon as the audit work is completed.

b. **Sensitive data—**examples include:

i. pre-publication reports in which there is press interest, or with significant impact on individuals, which are about wrongdoing, or which are politically sensitive;

ii. reports or letters drafted in response to a complaint.

Data of this kind may be stored on a WAO laptop for as long as it is being worked on, but must be deleted from the laptop once work is complete.

Staff must consider secure means of exchanging data of this type, for example, encrypted email, if the intended recipient is able to use this. Encrypted data sticks exchanged hand to hand are an acceptable alternative.

Ordinary, Internet email can be used if the intended recipient is not able to use encrypted email, and is content to accept the risk.

c. **Other data—**these are data not covered by the categories above and include, for example, general audit working information and minutes of meetings.

This type of data can be stored on laptops as required. Ordinary, Internet email can be used to acquire or exchange it.

16. Staff must make themselves aware of, and follow any specific requirements or policies an audited body has in place, for example, for documents which are protectively marked. If, however, an audited body's requirements appear to be unduly onerous so as to hinder audit access, staff should raise the issue with the Law & Ethics Manager.

Memory sticks (also known as USB sticks or drives)

17. Encrypted memory sticks, which require a password for access, can be used to transfer data between computers, or as a means of backup. These can be supplied by the IT team on request.

18. Ordinary, unencrypted memory sticks which do not require a password are an inherently risky way to store information and should never be used with WAO data.

Personal computers, smartphones and tablets

19. Staff may manage calendar appointments and email in their WAO account using personal equipment via the address for Outlook web access, email.wao.gov.uk.

20. Staff may connect personal smartphones or tablets to their WAO email/calendar account. To do this, search for the Hub article, "Using an Android or Apple smartphone with WAO email and calendar".

Backing up data

21. Information held on WAO systems and servers, for example, Insight, mailboxes inside Outlook email, and shared "network folders" are backed up using automated means. There is no need for staff to take specific backup action.

22. Staff must take steps to back up work, where the only up-to-date copy is on an individual's laptop. For example, at the end of a day during which a staff member has been updating a particular report, the latest version should be saved to a WAO server e.g. the "P drive", for example, or uploaded to the Insight system. This will guard against information loss in the event that the laptop fails, which can occasionally happen without warning.

23. Note that unlike the main mailbox, "personal folders" within Outlook, also known as .PST files, are **not** backed up to servers automatically. Staff should back these up manually if they are used.

Acceptable Use

24. Staff must not use WAO equipment in any way that may harm the organisation's reputation. For example, staff must not send, store or deliberately access material that:

a. is obscene or pornographic;
b. is likely to cause widespread offence;
c. is malicious, abusive or defamatory in nature;
d. is racist, sexist or otherwise constitutes unlawful discrimination in terms of protected characteristics defined by the Equality Act 2010 (i.e. in terms of age, impairment (disability), gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex (gender) and sexual orientation);
e. constitutes harassment.

25. Staff may use WAO equipment for personal purposes, for example, online banking, shopping or reading the news, provided the time spent doing so is a reasonably short "break from work".

26. Where personal use of WAO equipment incurs a cost, for example, personal calls on mobile or desk telephones, this must be limited to £5 per staff member per month or be reimbursed.

27. Staff may use social media, subject to the organisation's Social Media Policy, which can be found on the Hub. In general, staff should be aware that the rules and principles of conduct which govern the real world, also apply to the online world.

28. Staff must make themselves aware of, and follow any specific requirements or policies an audited body has in place when using its computers or systems.

Security Monitoring

29. WAO uses a range of monitoring techniques to ensure information and systems are properly protected, and that staff comply with WAO policies and the law.

30. WAO will ensure monitoring arrangements are reasonable and proportional to the risks.

31. Staff must accept that any use of WAO equipment, whether business or personal, may be recorded, scrutinised or investigated by these automated or manual means.

Reporting Security Incidents

32. Staff must report security incidents to the Information Security Officer. These could include instances where, e.g. staff of an audited body have sent personal and sensitive information via ordinary Internet email, or where a laptop has been stolen. Prompt reporting should enable corrective action to be taken and help WAO and other bodies to learn and make any necessary changes to avoid a repeat.

Getting Help

33. If you need advice on anything within this policy, or any practical aspect of working with information on WAO equipment, please contact the IT team on 02920 320690 or via email to “WAO ICT”.