ABERDEENSHIRE COUNCIL

ICT ASSET MANAGEMENT POLICY

PURPOSE

This Policy sets out a framework for the identification, management and control of computer hardware equipment and software assets in Aberdeenshire Council, including both corporate and curricular environments.

CONTENTS

EXECUTIVE SUMMARY

1. **This Policy should be read in conjunction with Aberdeenshire Council's Information Security Policy and associated Codes of Practice. These documents are available on Arcadia (under Our Council, Information Governance, Information Security). The main objectives of this policy are: -**

   - **To achieve best value by improved management information and resource planning during the lifecycle of ICT assets from procurement to disposal.**

   - **To ensure that Aberdeenshire Council complies with all relevant regulations and legislation and thus avoids the risk of prosecution.**

   - **To provide a comprehensive and easily understood framework for the identification and control of ICT assets.**

2. **This Policy will be implemented and maintained by a cross-Service ICT Asset Management Group reporting to the Information Security Management Group.**

3. **The ICT Service will provide a co-ordinating role and will collate and maintain an ICT Asset Register in partnership with all Council Services.**

4. **In line with Financial Regulations and associated guidelines, each school will also maintain an inventory.**

5. **Software will be acquired, identified, implemented and used in accordance with licence requirements and good management practice. Appropriate records will be kept during its lifecycle.**

6. **Hardware will be acquired, identified, implemented and used in accordance with good management practice. Appropriate records will be kept during its lifecycle.**

7. **The Council's Information Security Officer will lead a review of the Policy, as required. ICT will review the ICT Asset Register, as required.**

1.   Introduction

1.1   This Policy sets out the overall guidelines and procedures that apply to the identification, management and control of computer hardware equipment and software (ICT Assets) by employees and associated third parties of Aberdeenshire Council.

1.2   This ICT Asset Management Policy supplements Aberdeenshire Council's Information Security Policy.

1.3   Aberdeenshire Council is committed to the introduction and maintenance of effective ICT asset management practices in order to obtain best value from the assets through a rigorous system of management information and control. Achieving this also involves conforming to all legislation, regulations and computer software copyrights and adhering to the terms and conditions of any licence to which Aberdeenshire Council is a party.

1.4   The policy's main objectives are: -

- To achieve best value by improved management information and resource planning during the lifecycle of ICT assets from procurement to disposal. This may include transfer of excess assets between Services or Establishments.

- To ensure that Aberdeenshire Council complies with all relevant regulations and legislation and thus avoids the risk of prosecution.

- To reduce costs and improve productivity by enabling improved ICT services for deployment and support during the working life of an ICT asset.

- To contribute to the stability and security of Aberdeenshire Council's ICT environment.

- To inform and educate employees and associated third parties of their responsibilities while using Aberdeenshire Council's ICT assets.

- To inform and educate managers at all levels, and especially Directors, Heads of Establishments and other senior managers, of their special responsibility to endorse, promote and enforce the policy. Under related legislation, Directors, Heads of Establishments or other senior managers can be held individually responsible for breaches.

- To provide a comprehensive and easily understood framework for the identification and control of ICT assets in order to achieve and maintain compliance with the above objectives.

1.5   Aberdeenshire Council's ICT Asset Management Policy will be made available on Arcadia. It will be publicised, as appropriate, via the Core Brief, notice board displays and during induction processes.

2.   Scope

2.1   This Policy applies directly to the management of all Council ICT assets in both corporate and curricular environments.

3.   Associated Policies and Standards

3.1   The Aberdeenshire Council ICT Assets Management Policy aims to support: -

- The Council's Information Security Policy and associated Codes of Practice.

- The asset management principles defined by The Federation Against Software Theft (FAST).

- The Asset and Configuration Management best practice principles as defined in the BSI Code of Practice for IT Service Management/ITIL.

    For other related policies, codes of practice, legislation, regulations and directives see Appendix A.
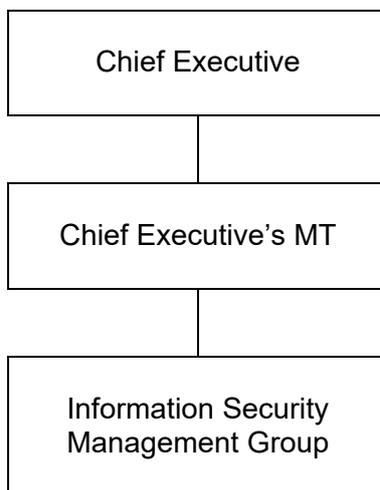
4.   Useful Terms and Definitions

Users	Council employees including teachers, temporary employees, elected members, learners, agency staff, contractors, third party employers and employees thereof, suppliers and any other party employed by the Council, who use ICT assets.
ICT Service	A shortcut term for the ICT sub-Service within the Council's Corporate Services Directorate.
ICT Asset Management	Management and control of all computer hardware and software, also incorporating accurate and up to date asset record keeping.
Information Security Management Group (ISMG)	A cross-Service group responsible for the implementation of this policy.
Service ICT Liaison Representatives	Persons within Services who are responsible for general liaison with the ICT sub-Service.
Service ICT Asset Representatives	Persons responsible within Services for maintaining an accurate record of all changes of description, user, location, status, etc. of computer hardware and software.
Compliance	Managing hardware and software within the constraints of our policy environment and the legal framework.
Software Licence Agreement	A legally binding contract between the software owner and user setting out terms and conditions of use. *For a quick guide to types of software licence agreement see Appendix B.*

Computer Virus   *'An unauthorised program that inserts itself into a computer system and then propagates itself to other computers via networks or disks; when activated it interferes with the operation of the computer.'*

5.   ICT Asset Management Organisational Framework

```
┌─────────────────────────────┐
│      Chief Executive        │
└─────────────────────────────┘
              │
┌─────────────────────────────┐
│    Chief Executive's MT     │
└─────────────────────────────┘
              │
┌─────────────────────────────┐
│   Information Security       │
│   Management Group          │
└─────────────────────────────┘
```

5.1   Key Organisational Responsibilities

5.1.1 The Chief Executive and Management Team
Have overall responsibility for commitment to and implementation of the ICT Asset Management Policy through their Heads of Service and management organisations. The MT will review and update the policy as necessary.

5.1.2 Information Security Management Group
The cross-Service group with high-level management responsibility for the implementation, maintenance and development of the Council's Information Security Policy in general and, in this context, the management of ICT assets.

5.1.3 ICT Asset Management Group
Designated staff from the ICT Service and all user Services. Has responsibility for day-to-day implementation, maintenance and development of the Council's ICT Assets Management Policy. Regular meetings will take place to co-ordinate implementation, monitor effectiveness and discuss development proposals. The following objectives will be addressed at each meeting of the ICT Asset Management Group: -
- To approve new initiatives to improve asset management.
- To review incidents of non-compliance.
- To assess the risk involved regarding incidences of unauthorised software, under and over-licensed situations etc.
- To ensure that the ICT Asset Management Policy is adopted as every day practice by all users of Aberdeenshire Council ICT assets.
- The group will review the legal, statutory, regulatory and contractual requirements that the Council, its suppliers and third parties, have to satisfy.

5.2   Asset Management Responsibilities

5.2.1   Head of Service ICT
Responsible for the overall operation of the centralised ICT asset management system. Reports, as required, to the Chief Executive's MT on ICT Asset Management policy and strategy issues. Accountable for achieving compliance of software licences.

5.2.2   ICT Services Team Leader (Transition)
Responsible for the allocation of resources and day-to-day line management control of a centralised ICT asset management system.

5.2.3   Principal Information Security Officer
Responsible for guiding the implementation, development and review of the Council's Information Security Policy. Will also initiate a review of the ICT Asset Management Policy and accuracy of the ICT Asset Register, as required.

5.2.4   ICT Staff
Where electronic auditing facilities are not available, ICT staff are responsible for updating the central ICT asset management system of installation, relocation or removal of computer equipment/software.

5.3   Service Asset Management Responsibilities

5.3.1   Heads of Service
Responsible for committing to and implementing the Council's ICT Asset Management Policy within their area of management control.

5.3.2   Heads of Establishment
Responsible for committing to and implementing the Council's ICT Asset Management Policy within their establishment.

5.3.3   Service ICT Liaison Representatives
Responsible for general liaison with the ICT Service including ICT asset management and related issues

5.3.4   Service ICT Asset Representatives
Jointly responsible with ICT for the day-to-day maintenance of the central ICT asset management system and ICT Asset Register and for ensuring that an accurate record of all changes of description, user, location, status, etc. of computer hardware and software is maintained.

6.   Inventory of ICT Assets
The ICT Service will collate and maintain an ICT Asset Register using, wherever possible, automated remote detection and identification facilities. Manual audits will be carried out on equipment not attached to the Aberdeenshire network. This will be achieved through the co-operation of and input from each Service via the Service users themselves, their Service ICT

Asset Representatives, Service ICT Liaison Representatives and all ICT staff involved.

The ICT Service is also responsible for providing, or enabling Services to generate for themselves, ICT asset inventory reports and associated management information to assist with meeting audit requirements and resource planning of ICT assets from procurement to disposal.

6.1   **Classification of ICT Assets**

The Council defines its ICT assets within the following groups: -

Covered by this policy	Not covered by this policy
Software Assets:	**Information Assets:**
Paper or electronic copy of software licence. Application software. Development software. Utility software. System software. Shareware, Freeware, Public Domain, Open Source, Adware, Spyware and Warez software, Games & Screensavers. Fonts (This is not intended to form an exhaustive list)	Databases Data files User manuals Technical Documentation System documentation Operational Procedures Support Procedures Archived Data, All media's Training Materials Disaster Recovery Plans Continuity Plans
Computer Hardware	**Utilities/Services Assets**

Desktop PC systems.
Laptop / Tablet / Netbook PC systems.
Server systems.
Inkjet printers.
Laser printers.
Plotters.
Multifunction Devices
(scanner/printer/fax/etc).
External storage devices
  (USB Hard Drives, USB Flash drives, etc).
Monitors
  (TFT, touch Screen etc).
Digital Cameras.
Routers, Switches and other computer associated communications equipment such as PBX's, Fax, answer machines and PDA's (Personal Digital Assistants) / Blackberrys
Any of the above in storage.
(This is not intended to form an exhaustive list)
	Computing and Communications Services.
	Heating services.
	Lighting services.
	Power services.
	Air conditioning services.
	Magnetic, optical (CD, DVD) media.
	Ancillary technical equipment.

7.   Software Asset Management

7.1   Software Licence Compliance

The process of compiling an accurate inventory of software assets is of utmost importance in achieving software compliance. Aberdeenshire Council must have the ability to provide proof of purchase for all software installed on their computer equipment.

Important information regarding software licensing: -

- The original licence agreement, original disks and associated 'receipted' invoices must be held on file in a secure location and be readily available for internal or external audit purposes and by software suppliers.
- The licence agreement certificate is the main document proving purchase of any software application.
- Where a piece of software has been upgraded, the original licence should be retained and stored with the upgrade licence.
- Purchase reports from suppliers and receipted invoices are valid proofs of purchase.
- Aberdeenshire Council users must adhere to the terms and conditions of the licence purchased. Failure to do so is the equivalent of having no licence. Seek guidance from the ICT Service if in doubt.
- "OEM licences" for the operating system and software applications that comes "bundled" with the hardware at the time of purchase cannot be transferred to other equipment in part or whole at any time.
- Site licences typically impose restrictions on software use.
- The majority of shareware, freeware, public domain, screensavers, games and other software available from the Internet require licence agreement certificates.
- Licences are required for all software applications installed on obsolete or stored computer equipment. This includes any 'hot swap' PCs that may be held in store as replacements for those utilised in critical systems.
- Membership of the Federation Against Software Theft (FAST) does not protect Aberdeenshire Council from litigation.

Benefits of achieving compliance: -

- Reduces the threat of legal action from software owners and suppliers (maximum penalty for non-compliance is 10 year imprisonment).
- Provides effective control of software and hardware assets.
- Identifies under/over licensing allowing for efficient use of licensed software.
- More efficient control of lease and hardware replacement, insurance and maintenance contracts and repairs under warranty.
- Lower cost of PC ownership.
- Improved security.

7.2   Normal Software Acquisition

All software required for use on Aberdeenshire Council computer systems <u>must</u> be procured in consultation with the ICT Service. This will allow the ICT Asset Management function to track and log the receipt of software applications and ensure that the correct licences are in place. Note section 7.5 below.

7.3   Emergency Software Acquisition

In the event of a genuine business requirement to obtain software urgently, contact must be made with ICT, as all software requirements must follow the ICT licence management procedures.

7.4   Software Installation

The installation of software applications onto Aberdeenshire Council's computer equipment is restricted to staff authorised by the ICT Service only. The software will be "packaged" for correct installation in the Council technical environment and "compliance tested" for compatibility with that environment.

Under no circumstances are software applications to be installed by unauthorised Aberdeenshire Council staff.

Following consultation with Service ICT Liaison Representatives, the ICT Service is empowered by this Policy to remove unauthorised software from Aberdeenshire Council ICT assets. A repeated failure to co-operate may lead to disciplinary action.

Contact the ICT Service Desk if in doubt (ext. 01224 664000 or int. 725 4000).

7.4.1   Games and Screensavers

Aberdeenshire Council does not permit the use of any screensavers other than those that form part of the standard computer operating system.

Games and screensavers may corrupt system configuration or performance, and will usually require a software licence. Use of games is not permitted within the corporate environment. Use of games is permitted within the curricular environment, where games have been legitimately acquired in order to support the curriculum.

Following consultation with Service ICT Liaison Representatives, the ICT Service is empowered by this Policy to remove unauthorised games and screensavers from Aberdeenshire Council ICT assets. A repeated failure to co-operate may lead to disciplinary action.

7.4.2   Fonts

No fonts can be downloaded and installed on an Aberdeenshire Council asset without discussing with ICT. Many fonts that can be downloaded incur a charge and require an appropriate licence.

7.4.3   Internet

Except where authorised by the ICT Service no software may be downloaded from the Internet. Users should not use any software received via email or any other Internet service.

Files to be particularly aware of are those with the following extensions; **.exe** (executable), **.bat** (batch files), .**com** (a command), **.pif** (programme information file) **.vbs** (Visual BASIC script) and **.zip** (WinZip files - these files

are not dangerous but may contain any of the files mentioned above). If in doubt contact the ICT Service Desk.

Where there is a genuine business case for the installation of software from the Internet this must be investigated and carried out by ICT Service.

The ad hoc installation of software from the Internet may put Aberdeenshire Council's systems at risk.

7.5   **Software Compliance & Documentation**
On completion of installation or update, all relevant media and licenses should be forwarded to ICT. The ICT Service will store centrally, in a secure fire resistant safe / location, all licences, 'receipted' invoices and original media. A software library is available on line with restricted access.

7.6   **Software Disposal**
The ICT Service will carry out (or arrange for a trusted third party to carry out) the removal of any redundant or under-utilised software applications installed on Aberdeenshire Council's or third party computer equipment. Software is owned by the Council, not by individual Services, and may , by agreement, be transferred between Services or between Establishments for the overall corporate good. Contact the ICT Service Desk so that the transfer or disposal of any software applications can be arranged on a timely basis.

7.7   **Adding & Removing of Software**
The addition and removal of software must involve the ICT Service. The ICT Service Desk must be advised of any change of configuration so that the ICT Asset Register can be updated.

8.   Hardware Asset Management

8.1   **Hardware Acquisition**
All computer hardware acquired by Aberdeenshire Council, including donations, must be obtained or procured in consultation with the ICT Service.

8.2   **Receipt of Hardware**
In order to be properly configured to Council standards all PCs and Laptops are to be delivered to the ICT Service. All hardware requirements must be requested through ICT by logging a request with the ICT Service Desk, which will ensure approved hardware is purchased. Deliveries of peripheral items such as keyboards and mice will typically be made directly to the relevant Service location.

8.3   **Hardware Installation**
Hardware will not be connected, installed or operated within Council properties without authority of the ICT Service.

Privately-owned hardware must not be connected, installed or operated under any circumstances – this includes privately-owned USB flash drives.

8.4   **Identification of Equipment**
Effective asset management relies on all computer equipment covered by this policy being identifiable via a unique asset numbering system. All equipment

valued at £100 or more or considered to be portable and desirable to a thief will be allocated the relevant asset number and an asset label attached (where physically possible) on or before installation. Some equipment, e.g. printers, with a value of less than £100 will also be included. Printers are key ICT assets and the volume utilised by Aberdeenshire Council warrants their inclusion in the ICT Asset Register. The ICT Service Desk must be advised if equipment is found not to have an asset label attached.

8.5   Hardware Security
To prevent the opportunist theft of unattended equipment it is recommended that all portable devices are stored, wherever possible, out of sight and preferably in a locked environment.

8.6   Hardware - Stolen or Damaged
It is essential that the user's line manager and Service ICT Liaison Representative be notified of any damage to or theft of computer equipment. Your Service ICT Liaison Representative will then log a call with the ICT Service Desk providing details of the incident.

If any personal data is lost, resulting from theft of hardware, the Council's Information Security Officer must be informed such that Data Protection implications can be fully considered.

8.7   Hardware - Change of User or Relocation of Equipment
The ICT Service Desk is to be advised of all changes to the users of or the relocation of computer equipment. All significant movement of ICT hardware must involve the ICT Service

8.8   Hardware Disposal
The ICT Service will oversee the removal of any redundant hardware installed in Aberdeenshire Council. - Hardware is owned by the Council, not by individual Services, and may be, by agreement, transferred between Services for the overall corporate good. There are significant logistical, environmental and information security issues associated with this work which will typically be undertaken by arrangement with trusted third parties. The costs of any disposal will normally be charged directly to the Council Services concerned. Contact the ICT Service Desk so that the disposal of hardware can be arranged on a timely basis.

8.9   Return of Unused ICT Equipment

Unused ICT equipment, particularly council laptops, must not be placed and stored in cupboards by services and left unused or forgotten. This practice creates a number of issues, in that it's not financially sound for the council to treat costly equipment this way, the equipment will not receive necessary updates, and if stolen it could present a threat to any confidential information stored on it.

Surplus equipment should be returned to ICT for redeployment to other users or securely decommissioned. Redeploying unused equipment reduces the need for the council to purchase or lease new equipment, and consequently reduces costs.

When out-of-date equipment is reconnected to the council network, because it has not received the necessary anti-virus updates it poses a

threat to network security. Please make sure you return equipment that is not being used so that updates can be installed and the risk of computer virus infections spreading is limited. Older equipment which has been sitting unused for any length of time may not be suitably protected with encryption software. This software ensures confidential information held on a computer is secure and without it the council could be faced with monetary penalties if important information is lost or stolen. The Information Commissioner has the power to impose a fine of up to £500,000.

9.   Other Issues Related to ICT Asset Management

9.1   Auditing of Networked Assets
Aberdeenshire Council electronically audits all computers periodically. Sample random audits may be carried out. Software monitoring may be conducted in specific circumstances in order to achieve and maintain compliance with this policy.

9.2   Standalone/Mobile/Laptop Users
Aberdeenshire Council's ICT Asset Management Policy applies to standalone, mobile and other users who do not log on to the Council's network and receive an automatic electronic audit. Where possible all such devices will be equipped with auditing software, however, users of such devices are responsible for contacting the ICT Service Desk to arrange for their ICT equipment to be manually audited on a periodic basis (at least once a year). In practice it is expected that an automatic reminder system will be developed.

9.3   Breach of Policy
All terms and conditions, as stated in this policy, are applicable to all Council employees including teachers, temporary employees, elected members, learners, agency staff, contractors and third party companies and employees thereof, and any other party employed by the Council.

Council Employees including Teachers
Should any Council employees deliberately or knowingly breach the terms of this policy, disciplinary action and/or appropriate legal action may be taken.

External Organisations
Should any agency staff, contractors and third party companies and their employees deliberately or knowingly breach the terms of this policy, appropriate contractual and or legal action may be taken.

Elected Members
Should any elected member of the Council deliberately or knowingly breach the terms of this policy, the matter will be referred to the Chief Executive for further action.

Learners
Should any learner deliberately or knowingly breach the terms of this Policy, the matter should be referred to the Head of the Establishment or other appropriate Senior Manager.

9.4   Review of ICT Asset Management Policy
The Information Security Officer will review the Policy as required in conjunction with appropriate representatives from each Service. Appropriate action will be taken should amendments be required.

APPENDIX A – Associated Policies, Legislation, etc.

Policies and Codes of Practice

Existing Aberdeenshire Council Policies & Codes of Practice: -

- Information Security Policy.
- Acceptable Use Policy and associated Codes of Practice.
- Data Protection Policy and associated Code of Practice.
- Monitoring and Investigation of ICT Facilities Code of Practice
- The EL&L Email Protocol
- Remote Working Code of Practice
- Organisation of Information Security Code of Practice
- Using email efficiently Guidance.
- Disciplinary Policy, Procedure and Guidance for Managers.
- Policy – Disclosure of Information (Whistleblowing).
- Environmental Charter
- Financial Regulations

Legislation, Regulation, Directives and Codes of Practice

- The asset management principles defined by The Federation Against Software Theft (FAST)
- The Asset and Configuration Management best practice principles as defined in the BSI Code of Practice for IT Service Management/ITIL.
- BS ISO/IEC 17799 (2005) Part 1 'Code of Practice for Information Security Management'.
- The Copyright, Designs & Patents Act 1988.
- Copyright (Computer Programs) regulations 1992.
- Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002.
- Computer Misuse Act 1990.
- Data Protection Act 1998.
- Trade Marks Act 1994.
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A).
- Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.
- Waste Electrical and Electronic Equipment Directive.
- Uniform Computer Information Transaction Act.
- The Telecommunications (Data Protection and Privacy)(Direct Marketing regulations 1998.
- Obscene Publications Act 1959 & 1964.
- Protection of Children (Scotland) Act 2003.
- Consumer Protection (Distance Selling) Regulations 2000.
- Defamation Act 1996.
- Electricity at Work Regulations 1989.
- Electronic Communications Act 2000.

APPENDIX B – Software Licence Agreements

Software Licences	There are many types of licence agreement available. At its most basic level it is a legally binding contract between the software owner and user setting out terms and conditions of use. It is the responsibility of the user to read, understand and comply with the terms and conditions stated on the licence. In a standard software licence agreement the user purchases the right to use the software on their systems while the copyright holder retains ownership.
Shareware	Shareware is software that is distributed by the copyright holder to allow users to evaluate it through day-to-day use. A trial period is normally granted for use, after which the user is expected to pay for the software or delete it from their computer systems. Shareware is bona fide copyright protected software and should not be used without a licence.
Freeware.	Freeware is owned by its author but is supplied free of charge but may be subject to restricted use. It can be copied, distributed and developed in a non-profit making and non-commercial manner. A large proportion of Freeware is subject to the GNU (General Public Licence).
GNU (General Public Licence)	Type of licence used by software authors to ensure that users have freedom of use of their software with no legal limitation to copying, distribution, modification etc.
Adware & Spyware	Adware is Shareware & Freeware that displays advertisements. Spyware is Adware that monitors PC usage and reports back to an email address or web site, usually without the users knowledge.
Fonts	Fonts outwith those that are provided along with an application often requires a separate licence to be purchased.
Public Domain.	The owner of the copyright does not enforce any rights to the software. It can be used for any purpose including commercial.
Warez	Software made available illegally, usually with its copy protection removed.
Open Source	Copyright protected software made available to the public without licence restrictions that limit its use, modification or redistribution. This may or may not be supplied free of charge.

POLICY

Revision Date	Previous Revision Date	Summary of Changes
14th May 2015	February 2013	Revision and Distribution sections added.
February 2013	-	Merge of Corporate and EL&L Asset Management Policies

DISTRIBUTION

The approved versions of these documents are distributed to:

Name	Title
Arcadia	Our Council/Information Governance/Information Security

Any copies of these documents out with the distribution list above is uncontrolled.