ICT Purchasing Policy

Document Information

Project Name	ICT Purchasing Policy
Version	007
Status	Final
Date	27/10/2014 (reviewed 23/2/2018)
Classification	Unclassified

Purpose

The purpose of this document is to detail the Councils IT software, hardware & services purchasing policy. In conjunction with the ICT Purchasing Standards, It provides the requirements and information for software installations within Ashfield District Council from a technical and security standpoint. This policy will be referenced by a top level Governing Policy.

Distribution

Copy to	ADC employees, 3rd Party suppliers, Council Members

Document History

Version	Date of Production	Version Description	Author
00a	5/1/2009	First Draft	RW
00b-d	7/1/09-25/1/09	Amended to include new general section that shows requirement of consultation with I.T and the need for staff to make sure suppliers agree to the policy. Rewritten to remove ambiguity. Amended following comments by IM (Audit)	RW
001	11/2/09	Status changed to Final	RW
002	17/2/09	Add general statement about I.T. engagement	RW
002b	16/11/09	Rename policy, inc. agreement of timescales and make sure it lines up with the ICT Technical Strategy.	RW
002c	19/5/10	Add specific reference to freeware and open source products	RW
003	16/6/10	Add additional security requirements and change status to final	RW
003a	3/9/10	Policy split into an unclassified policy and a Protected standards document.	RW
004	20/12/2010	Approved at full Council and made final.	RW
004a-c	11/08/2011-8/12/2011	Expand free software statements following audit recommendation Add requirement to consult with or inform DPO if the software involves personal data. Add possible approval by group chaired by I.T.	RW
005	13/2/2012	Made final	RW
005a	5/11/2012	Add reference to hosted service policy	RW
006	1/8/2013	Made Final	RW
007	27/10/2014	Add reference to joint dev group	RW

Key Personnel

Author	Russell Wheatcroft	
Editor/s	Andy Slate	
Owner	Russell Wheatcroft	

Contents

1. Introduction

Who does this policy apply to?

- ADC Employees
- 3rd Party suppliers of software/systems

Why have a Software Purchasing Policy?

- To ensure that software can be supported by existing resources and documented procedures
- To allow centralized control of all software for ease of installation and to speed up the process of upgrading or patching
- To ensure software is installed in such a way that does not require the relaxing of security or impact on other systems.

2. General

- A more detailed list of requirements will be documented in the ICT Purchasing Standards, which will be approved at Senior Management Level.
- Internal staff are not expected or required to fully understand the associated ICT Purchasing Standards but they are required to make sure that software suppliers indicate their understanding and acceptance of the Standards. If any clarification is required, this should be discussed with I.T.
- All IT software, hardware and services should be approved by I.T. or a group containing a senior ICT employee prior to purchase with appropriate consultation for Legal and Security matters (for example, correct use of data or data security).
- All large or key systems (including projects with a reasonably large financial investment) will require the submission of a project brief using an agreed template as part of the approval process,
- Timescales for the installation of software, hardware or systems should be agreed in advance with I.T.
- I.T. should be engaged as early as possible when considering the purchase of new software or systems.
- Business cases should be created and approved for new software.
- Proper contractual arrangements for software support should be considered.
- The Council will ensure there is appropriate provision for access controls within the system. For example, there should as a minimum be a distinction between an administrator user and a normal user.
- A guarantee should be sought from the supplier of any software that they do not have a higher level of access to the system that that of the Councils' System Administrators.
- Consideration should be given to the ICT Password Policy/Standards and relevant aspects should be agreed with the supplier.

- Freeware, shareware and open source products will be considered for use based on suitability and risk.
- Licensing restrictions on free products will be reviewed to check suitability in a corporate environment and to ensure installation is not limited to personal use.
- I.T. may request the nomination of an internal Asset/Data Owner (Usually 3rd tier or above) and a lead administrator following purchase depending on system content and method of access to system.
- The Councils Information Officer (commonly referred to as the Data Protection Officer or DPO) should be consulted/informed if the Purchase involves the processing of personal data.
- If a proposed system is to be hosted outside the Council's data environment then it must be also compliant with the "ICT Hosted Service Policy". The statements in this Policy are still valid for PC software and Web Front End.

3. Server Software

- All data needs to be stored on servers and not on PCs.
- All server components must be installed on the servers and not on a local pc
- The Council will document a preference for the database software used in the ICT Purchasing Standards but others may be considered at the discretion of I.T.
- Unlike PC installations, any server side installation/configuration can be carried out manually.
- All server software should be capable of running in a virtualized server environment.
- A requirement for the supplier to provide Project Management should be considered depending on the Size, complexity and Integration of the system
- All 'Larger' or 'Key' installations should have a Post Implementation Review
- Any communication with the server from outside the internal network must be carried out in a secure manner with appropriate encryption and security controls.
- Any server software must be configured and patched to a level of acceptable risk when assessed using industry standard vulnerability scans, both externally and internally

4. PC Software

- Software is not installed directly onto PCs within the Council, but is remotely distributed centrally by Active Directory Group Policies or

SCCM. Assistance would be expected, if required, from the supplier to prepare the software for deployment.

- Installation and training should not be on the same day, as the preparation and testing for deployment could take more than a day.
- ALL users have minimum “rights” on the PC (NOT administrator or Power User rights). If modification is required to allow access to certain registry keys or folders, these changes would be added into the “distribution”. Assistance would be expected, if required, from the supplier to identify these permission changes
- Software should not have Individual licenses for each copy installed, as this makes it is impossible to create one distributable copy.
- If plug-in devices are required as part of using the software (e.g. license “dongles”, barcode readers, remote controls etc) then this should be achievable without the requirement for an administrator login.
- It is acceptable that software is simply copied to a network drive and run straight from the network drive. The Council would distribute the shortcut to the software via a group policy.
- Printing should be to standard windows networked printers and not, for example, USB.
- Each piece of PC software should be standardised on one version to minimize problems with usage across the Authority and software patching.
- Exceptions to the above procedures following an assessment of risk and practicality, are at the discretion of I.T.

5. Web Front End Software

If access to a system is via a web browser, either to an external website or to an internal website hosted on one of the Councils servers, then the following policies come into effect.

- The Council standardises on Internet Explorer and Google Chrome which are available on all PC. The exception to this is mobile devices.
- There should not be a requirement to change any security settings to connect to a web service that may put the Councils network at risk.
- ActiveX should be avoided but if there is a requirement to use ActiveX as part of the system, then there are extra requirements.
    a. The Council does not allow users to install ActiveX as this is a security risk.
    b. ActiveX installations will be distributed to the PCs. Assistance would be expected from the software supplier in the preparation of this deployment.
    c. If the website is held externally, then the council would require advance notice if ActiveX’s are going to be changed, so that preparation of a new deployment can be made as soon as possible to minimize downtime.

- Exceptions to the above procedures, following an assessment of risk and practicality, are at the discretion of the I.T section.