# Gloucestershire County Council
# Software Management Policy

## 1.0 Policy Statement

1.1 Gloucestershire County Council (the Council) will ensure the acceptable and legal use of software by all users of the Council's computer equipment and Information Systems.

## 2.0 Scope

2.1 The Software Management Policy applies to all councillors, employees, partners, contractors and agents of the Council (referred to as users) who have access to council computer equipment or information systems with the exception of the Gloucestershire Fire and Rescue Service and Gloucestershire Schools.

2.2 All software in use on council computer equipment or to run council information systems is covered by this policy with the exception of council supplied equipment that is provided to clients such as Foster Carers.

2.3 If you do not understand the implications of this policy or how it may apply to you please seek advice from please the ICT Service Desk.

## 3.0 Risk Management

3.1 The Council acknowledges that there are risks associated with the use of software within the Council but that the use of software is critical for the efficient running of the Council.

3.2 This policy seeks to mitigate the following risks:

- Harm to individuals
- Viruses and other malicious software (malware)
- Service disruption
- Inappropriate use of council resources
- Legal non-compliance and/or fines
- Damage to the Council's reputation

## 4.0 Responsibility for Software

4.1 All software must have an officer with responsibility for that software i.e. the "Information Asset Owner". A register of Information Asset Owners can be found at http://gccwebapps/BusinessApplicationsCatalogue/

4.2 The Information Asset Owner may delegate some responsibility for the management of the system to a System Administrator. However, for the purpose of this document, the responsibility remains with the Information Asset Owner. Further information on Information Asset Owner and Manager roles can be found at the IAO Help & Guidance page.

## 5.0 Software Acquisition

5.1 All software acquired for use on council computer equipment must be purchased through the ICT Service Desk. This is to ensure:

- that the Council has a complete record of all software that has been purchased and can register, support and upgrade this software accordingly
- legal compliance
- the software is fit for purpose
- the acquisition is properly procured with appropriate authorisation.

5.2 Software available for download via the Internet must only be purchased and/or downloaded by the ICT Service.

5.3 Personal or unsolicited software, including screensavers and games must not be loaded onto a council machine as this may result in the Council infringing its legal obligations, or malicious code (e.g. a virus) being introduced into the Council's ICT environment.

5.4 All software purchased for council use must be registered in the name of the Council and/or the directorate. Software must not be registered to an individual.

5.5 Software acquired for use within the Council will only be used in accordance with the licence agreement. It is the Information Asset Owner's responsibility to ensure the Council is compliant with the licence conditions.

5.6 Copying of software is a breach of the Copyright, Designs and Patents Act (1988) and is not permitted.

## 6.0 Software Inventory

6.1 The ICT Service will maintain a complete inventory of all software in use within the Council and will retain the original media. All media must be passed to ICT for storage and must not be held by staff.

6.2 As a minimum the software inventory will record the following details:

- The title and publisher of the software
- Date and source of the software acquisition
- The software product's serial number
- The number of licences acquired by the Council
- Support and maintenance details

## 7.0 Software Installation

7.1 Software (including Shareware, Freeware and Public Domain software) must only be installed by the ICT Service. For software installation contact the ICT Service Desk.

7.2 Software will be installed by the Council's software deployment system, unless it is impractical to do so.

7.3 It is the Information Asset Owner's responsibility to ensure that the Council has acquired sufficient licences to cover the number of installed copies.

## 8.0 Software Support

8.1 All software must be supported by the supplier. This may be in the form of:

- 'off the shelf' software support from the supplier, such as Microsoft, or
- a more tailored software support and maintenance contract taken out between the Council and the software supplier, or
- a contract between the Council and a 3rd party for the support of a software package or application.

8.2 Where a support contract is in place between the Council and a software supplier or 3rd party, the Information Asset Owner must ensure that the contract remains current and up-to-date, that they are familiar with the terms and conditions of the support arrangements.

8.3 Supplier support must include the provision of 'patches' to fix known issues or security weaknesses that come to light during the lifetime of the software. Where this is not provided it will be recorded on the Software Risk Register and the Information Asset Owner must put a plan in place to replace the software with an alternative product that is both supported and patchable. The ICT Service will maintain the Software Risk Register and report to the Information Board as appropriate.

8.4 Where there is a business requirement for Open Source or Freeware products, the ICT Service must be consulted to ensure that adequate support arrangements are in place for the software. Contact the ICT Service Desk.

## 9.0 Patch and Upgrade Management

9.1 Information Asset Owners and the Council's ICT service are responsible for ensuring that Council software is appropriately patched, supporting information/guidance for Information Asset Owners is provided at https://staffnet.gloucestershire.gov.uk/internal-services/information-management-security-governance/information-asset-owners-iao-help-guidance/; for additional advice please contact ICT Service Desk.

9.2 Risk assessment must form the basis for prioritisation, testing and deployment of security updates. Any emergency or critical security patches issued by the supplier must be promptly applied in accordance with ICT emergency/critical patching procedure. Other security patches will be applied in accordance with the ICT

patching schedule at https://staffnet.gloucestershire.gov.uk/internal-services/the-ict-service/other-ict-services/ict-service-status/planned-outages-and-changes/ and the GCC Patch Management Procedure.

9.3 For other non-critical patches, the Information Asset Owner must produce a policy of when patches will be applied. For 'line-of-business' applications (e.g. ERIC or SAP) a bi annual or annual patching schedule may be appropriate, guidance is provided at https://staffnet.gloucestershire.gov.uk/internal-services/information-management-security-governance/information-asset-owners-iao-help-guidance/http:/gccwebapps/BusinessApplicationsCatalogue/. For additional advice and to ensure patches are applied in a controlled manner contact ICT Service Desk.

9.4 Patches may be rolled up by the supplier into a version upgrade. Only supplier supported versions of software will be used. Where the software forms part of an application, version upgrades should be included in the application roadmap. For each application Information Asset Owners are responsible for producing and maintaining an application roadmap, for advice contact the ICT Service Desk

9.5 All upgrades will be applied in a controlled manner with adequate acceptance testing undertaken by experienced users before the upgrade is released to all users of the software.

9.6 There is sometimes a complex relationship between the application software, the database management system, and the underlying operating system. All these components must be fully supported and patched. Where this is not possible the software must be included on the Software Risk Register and a mitigation plan put in place to move to supported versions of all components.

## 10.0 Software Development

10.1 Software must not be changed or altered unless there is a clear business need. A procedure must be in place that ensures: all software changes are approved, change requests consider whether the change is likely to affect existing security arrangements, and there is a record of all changes. Development Controls Guidance is provided at https://staffnet.gloucestershire.gov.uk/internal-services/information-management-security-governance/information-asset-owners-iao-help-guidance.

10.2 It is the Council's policy to purchase 'off the shelf' packages rather than develop software in-house.

10.3 Some in-house development does still take place (e.g. the Adult Social Care System and Microsoft Access databases). All such in-house development is to be used for council business purposes only.

10.4 The Information Asset Owner must ensure that intellectual property rights for in-house developed software remain with the Council and not the individual(s) or company that developed the software.

## 11.0 Documentation and Training

11.1 All software in use must be documented. This may take different forms, including but not limited to:

- System documentation
- User manuals
- Online help and/or documentation
- On-line training packages

11.2 The Information Asset Owner is responsible for ensuring up-to-date documentation is available, and that adequate training is available to staff.

## 12.0 Software Retirement

12.1 When software reaches the end of its useful life it must be handled in a controlled manner and in accordance with the terms of the software licence. The Information Asset Owner is responsible for:

- Ensuring that where a support/ maintenance contract is in place, notice is given to the supplier to cease the contract in line with the terms and conditions of the contract.
- Providing details to the ICT Service who will ensure the software inventory is updated accordingly, contact the ICT Service Desk
- Ensuring that the data processed by the software is archived, migrated to a new application, or removed and destroyed securely in conjunction with the ICT Service, contact ICT Service Desk.

12.2 The software will be removed from any council computer equipment by the ICT Service.

## 13.0 Policy compliance

13.1 According to the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties; the Council does not condone the illegal duplication of software.

13.2 All employees, and anyone who delivers services on the Council's behalf e.g. contractors, partners, agents or other third parties with access to the Council's information assets have a responsibility to comply with this policy which can be found at Information Management and Security Policies, and to promptly report any suspected or observed security breach; further details are provided at https://staffnet.gloucestershire.gov.uk/internal-services/information-management-security-governance/information-security-breaches-and-concerns/.

13.3 Security breaches that result from a deliberate or negligent disregard of any security policy requirements may, in the Council's absolute discretion, result in disciplinary action being taken against that employee. In the event that breaches arise from the deliberate or negligent disregard of the Council's security policy requirements by a user who is not a direct employee of the Council, the Council shall take such punitive

action against that user and/or their employer as the Council in its absolute discretion deems appropriate.

13.4 The Council may, in its absolute discretion refer the matter of any breach of the Council's security policy requirements to the police for investigation and (if appropriate) the instigation of criminal proceedings if in the reasonable opinion of the Council such breach has or is likely to lead to the commissioning of a criminal offence.

## 14.0 References

14.1 This policy and other related information security policies, standards and procedures can be found at Information Management and Security Policies.

## 15.0 Review and Revision

15.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

## 16.0 Key Messages

- All software must be purchased through and installed by the ICT Service.
- Personal or unsolicited software must not be installed on a council machine.
- All software must have a licence, and be used in accordance with the licence conditions.
- Information Asset Owners must put in place patching policy to minimise the risk associated with vulnerabilities.
- Unpatchable software should not be used.
- Unauthorised changes to software must not be made.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

## Document Control

| | |
|---|---|
| **Author:** | Julia Evans, ICT Infrastructure Manager<br>Sue Blundell, Information Security Advisor |
| **Owner:** | Andrew McCartney Programme Director |

**Revision History** Date of next revision: November 2015

| Revision date | Previous revision date | Summary of Changes | Changes marked |
|---|---|---|---|
| Jan 2010 | n/a | First draft | v0.1 |
| May 2010 | Jan 2010 | Including amendments | v0.2 |
| Aug 2010 | May 2010 | Including amendments | V0.3 |
| Oct 2010 | Aug 2010 | Including amendments | V0.4 |
| Dec 2010 | Oct 2010 | Including links, supporting advice & guidance | V0.5 |
| Feb 2011 | Dec 2010 | 2 minor changes | V1.0 |
| Jan 2012 | Feb 2011 | Align all Information Security Policy review dates to Nov 2012 as agreed by Information Board 26/9/2011 | V1.1 |
| Nov 2012 | Jan 2012 | Amendments contacts to take account of the new ICT structure. Change Information Asset/Systems Owner to Information Asset Owner. Amend links to business applications database | V1.2 |
| October 2014 | November 2012 | Amendments to reflect the changes in the ICT service and the introduction of an ICT patching schedule and procedure. Update links to Staffnet pages. Remove Appendices re Development Controls guidance and Patching guidance for IAOs for publishing on IAO Staffnet page | V1.3 |
| December 2016 | October 2014 | Updated links to take into account new ICT pages on staffnet | V1.4 |

**Distribution** This document has been distributed to:

| Name | Title | Date of Issue | Version |
|---|---|---|---|
| Julia Evans | ICT Infrastructure Manager | Oct 2009 | v0.1 |
| Andy Gilbert | ICT Technology Manager | Apr 2010 | v0.2 |
| Anne Mankin | ICT Software Compliance & Licensing Officer | Apr 2010 | v0.2 |
| Ron Sparrow | ICT Client Liaison Manager | Apr 2010 | v0.2 |
| Michelle Jones | ICT Client Liaison Manager | Apr 2010 | v0.2 |
| Sue Blundell | Principal IT Auditor | May 2010 | v0.2 |
| Will Felgate | Senior Lawyer | May 2010 | v0.2 |
| Anne Mankin | ICT Software Compliance & Licensing Officer | Aug 2010 | v0.2 |
| Sue Blundell | Information Security Advisor | Oct 2010 | V0.3 |
| Michelle Jones | ICT Client Liaison Manager | Oct 2010 | V0.3 |
| Anne Mankin | ICT Software Compliance & Licensing Officer | Oct 2010 | V0.3 |
| Sungard | John Baker | Oct 2010 | V0.3 |
| Information Board | N/A | Nov 2010 | V0.4 |
| Information Board | N/A | Feb 2011 | V0.5 |

**Document Approvals**

| Version | Approved By | Date |
|---|---|---|
| V1.0 | Information Board | April 2011 |

| | | |
|---|---|---|
| V1.1 | Information Board | 26/9/11 |
| V1.2 | Information Board | 19/12/2012 |
| V1.3 | Information Board | 16/10/2014 |