Software Management Policy

1.0 Policy Statement

Gloucestershire County Council (the council) will ensure the acceptable and legal use of software by all users of council's devices or information systems. The council will also ensure that appropriate measures are in place to safeguard its networks (GCC's and accessed by the public mainly in Gloucestershire Libraries) and any associated hosted software.

2.0 Risk Management

The council uses a range of approved applications to deliver services to customers. Up to date, correctly licenced software is critical for the safe and efficient delivery of services.

This policy aims to ensure appropriate protection, use and management of software within the council's networks and on council devices, which will help to mitigate the following risks:

- Harm to individuals;
- Damage to the council's reputation;
- Potential legal action and/or fines against the council or individual(s);
- Inappropriate use of council resources;
- Viruses and other malicious software;
- Service disruption;
- Procurement of software where an equivalent alternative is already available;
- Duplicate applications being used for the same purpose.

3.0 Scope

This policy applies to all employees, partners, contractors, Members, agents of the council and other third parties ('users') who have access to or are responsible for, the Council's networks and/or information systems.

This policy applies to all software used for GCC business purposes. If you do not understand the implications of this policy or how it may apply to you, you should raise a request via ServiceNow.

4.0 Responsibility for software

There are a number of roles within the council with responsibility for the management and day to day administration of software, these roles include but are not limited to:

- System Owners, who are accountable for ensuring sufficient user licencing is in place and are responsible for informing the ICT Service of any changes in system ownership, administration or contract management roles;
- System Administrators, who are responsible for the delivery of tasks as permitted by the System Owner, such as system configuration, user access controls and the day-to-day management of the system;
- Contract managers, who are responsible for ensuring that all systems have a current support and maintenance contract in place.

Budget holders, who are responsible for ensuring that the software acquisition and maintenance costs are within their allocated budget and take into account the total cost of ownership, including any potential cost increases due to inflation, licensing fees, support contracts, or upgrades.

5.0 Software Acquisition

All software acquired for GCC business purposes must be requested through ServiceNow prior to purchase. This is to ensure:

- necessary security and compatibility checks have been undertaken.
- a complete record of all software purchased is in place, which is registered, supported and upgraded accordingly;
- legal compliance;
- the software is fit for purpose;
- the acquisition is properly procured with appropriate authorisation;

Software available for download via the Internet must only be purchased and/or downloaded by the D&ICT Service.
The D&ICT Service must be consulted prior to procurement of all software.
When procuring software, contract managers should always consider the option of purchasing cloud hosted products and services where possible.
Software used within the council must be in accordance with the licence agreement. It is the System Owner’s responsibility to ensure the council is compliant with the licence conditions.

Copying of software is a breach of the Copyright, Designs and Patents Act (1988).

6.0 Software Inventory

The D&ICT Service will maintain a complete inventory of all software in use within the council and will retain the original media. All original media must be passed to D&ICT for storage.

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;
- The intended purpose of the software;
- Name and job title of System Owner, System Administrator(s) and Contract Manager.

7.0 Software Installation

Software must only be installed onto GCC managed devices by the D&ICT Service. For software installation, contact the ServiceNow.

Locally hosted software will be installed by the council's software deployment system, unless it is impractical to do so.

8.0 Software Support

All software must be supported by the supplier. These support agreements must include:

- System Security (i.e. patching and updates);
- System functionality improvements;
- System failure and support;
- Business continuity and disaster recovery details as applicable.

Any manager with responsibilities for software must ensure they follow corporate contract management and information asset owner guidelines.

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. All software must be in support from the vendor or support partner. Software that is not supportable is a risk to GCC, and a plan should be in place to replace the software with an alternative product that is both supported and patchable.
Where there is a business requirement for Open Source or Freeware products, the D&ICT Service must be consulted to ensure that adequate support and licencing arrangements are in place for the software. Please raise a support ticket in ServiceNow to ask for more information.

9.0 Patch and Upgrade Management

System Owners and the council's D&ICT Service are responsible for ensuring that software is appropriately patched, for additional advice please contact ServiceNow

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.

For other non-critical patches, the System Owner must produce a policy of when patches will be applied. For 'line-of-business' applications (e.g. SAP) a biannual or annual patching schedule may be appropriate. For additional advice and to ensure patches are applied in a controlled manner contact ServiceNow.

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 System Owners are responsible for producing and maintaining an application roadmap, for advice contact the ServiceNow.

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. Software should be kept up to date with an upgrade schedule that ensures the council is on the current latest version or current latest version -1.

10.0 Software Development

Software must not be changed or altered unless there is a clear business need. A procedure must be in place that ensures that 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. For guidance on change enablement please contact refer to Information Asset Owners (IAOs) – overview of your responsibilities on StaffNet.

The council will purchase 'off the shelf' packages rather than develop software in-house. In-house development will only take place where no suitable 'off the shelf' package is available. Suitability will be measured against business outcomes and in-house development only considered where existing software does not meet 80% of the required functionality. All such in-house development is to be used for council business purposes only.

System Owners 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 Software Security

Information Asset Owners and the ICT Service are responsible for ensuring that software is securely managed.

System Owners must ensure all software is configured and managed in line with applicable security policies including:

- Information IT Access Policy
- GCC Password Policy

System Owners must ensure all systems/software have event audit logging enabled.

All new software must undergo a security assessment before installation on the council's networks or devices. There may be a charge for this service which should be budgeted for. For more information contact the ServiceNow

12.0 Documentation and Training

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;
- Training packages.

System Owners are responsible for ensuring up-to-date documentation is available, and that appropriate training is available to staff.

13.0 Software Retirement

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 System 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 ServiceNow.
- 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 ServiceNow.

The software when no longer licenced will be removed from any council device by the ICT Service.

14.0 Policy compliance

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.

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.

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.

15.0 References

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

16.0 Document Control

16.1 Document information

Owner:	Assistant Director: Digital & ICT
Author:	IMS and ICT Policy Group
Reviewer:	IMS and ICT Policy Group
Board(s) consulted:	
Date created:	December 2010
Next review date:	December 2025
Approval:	Information Board, July 2021 (v2.0)
Date of approval:	

Scheme of Delegation ref:	
Version:	2.3
Classification:	UNCLASSIFIED

16.2 Version History

Version	Version date	Summary of Changes
2.0	June 2021	Full policy review
2.1	January 2023	Accessibility review and updates to formatting. Broken links fixed.
2.2	July 2024	Group policy review and broken links fixed.
2.3	September 2024	Minor changes completed, full policy review scheduled for end of 2025 in line with Digital and ICT Service Design.

16.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

16.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: dpo@gloucestershire.gov.uk

Phone: 01452 324000