Gloucestershire County Council
Software Management Policy

1 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 People's) and any associated hosted software.

2 Risk Management

The council uses a range of approved applications to deliver services to customers. Up to date, legally 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;
- Duplicate applications being used for the same purpose.

3 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 application software hosted on GCC managed devices. If you do not understand the implications of this policy or how it may apply to you please seek advice from the ICT Service Desk.

4 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.

5 Software Acquisition

All software acquired for use on the council's networks and on council managed devices must be authorised through the ICT Service Desk. This is to ensure:

- 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;
- necessary security and compatibility checks have been undertaken.

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

When procuring software, contract managers should always consider the option of purchasing cloud hosted products and services where possible.

Personal or unsolicited software must not be loaded onto any council device, 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.

Software used within the council must only be used 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 Software Inventory

The 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 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 Software Installation

Software must only be installed by the ICT Service. For software installation, contact the ICT Service Desk.

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

8 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.

Where a support contract is in place between the council and a software supplier or 3rd party, the Contract Manager must ensure they are aware of the terms and conditions of the support arrangements.

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 System 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.

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

9 Patch and Upgrade Management

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

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 and the GCC Patch Management Procedure. The criticality of a patch will be reviewed using the published CVSS score.

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 bi annual or annual patching schedule may be appropriate. For additional advice and to ensure patches are applied in a controlled manner contact ICT Service Desk.

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 ICT Service Desk

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

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 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. Associated guidance is provided at Development Controls Guidance.

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 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 software has 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 ICT Service Desk.

The ICT Service will ensure that the council's networks are adequately protected. This will include:

- The installation of network wide malware protection software;
- Network event logging and monitoring to identify potential threats.

11 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 adequate training is available to staff.

12 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 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.

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

13 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.

14 References

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

15 Review and Revision

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

Document Control

Author:	IMS/ICT policy group
Owner:	Karl Grocock – Assistant Director Digital and ICT

Revision History Date of next revision: July 2024

Revision date	Previous revision date	Summary of Changes	Changes marked
June 2021	December 2016	Full policy review	2.0

Document Approvals

Version	Approved By	Date
2.0	Information Board	July 2021