information management & security

Gloucestershire COUNTY COUNCIL

Joiners, Movers, Leavers (ICT) Policy

1.0 Policy Statement

Gloucestershire County Council (the council) understands that a robust joiners, movers, and leavers process is essential in enabling the council to safely and securely manage and control its data assets.

This policy ensures the management of joiners, movers, and leavers across the ICT estate. The principal drivers for an effective Joiners, Movers, and Leavers (JML) policy are:

- **Access Management:** Ensuring the council network and information resources can only be accessed by authorised persons.
- **Asset Management:** Ensuring the Digital and ICT Service has accurate knowledge of asset ownership, location, and status.

This policy aims to ensure:

- all individuals have appropriate access to the information needed to deliver the council's objectives and understand their responsibilities in safeguarding the council's physical and digital information assets.
- the appropriate confidentiality, integrity, and availability of those assets.
- unauthorised access to assets and/or information is prevented.
- the device estate is effectively managed by the Digital and ICT Service, ensuring confidentiality is maintained.

2.0 Scope

This policy applies to all joiners, movers, and leavers with access to the council's assets, including but not limited to, council owned devices and peripherals, all ICT software and systems used by council staff and all information assets (including but not limited to, paper and electronic records, voice conversations, photographs, videos, and CCTV footage).

For the purposes of this policy, Joiners, Movers, and Leavers are defined as follows:

- Joiners are individuals who require new access to the council's information systems/assets as part of their role.
- Movers are individuals who already access the council's information systems/assets and are transferring to a different role within organisation.

- Leavers are individuals who are leaving the organisation and are no longer entitled to access the council's information systems/assets.

This policy also applies to subcontractors and third parties working for or on behalf of the council, who are authorised to access the council's information in the course of their work.

3.0 Responsibilities

The Assistant Director: Digital & ICT has overall responsibility for the effective operation of this policy. Responsibility for monitoring and reviewing this policy and making any recommendations for change to minimise risk, lies with the Senior Information Risk Owner.

If you do not understand the implications of this policy or how it may apply to you, you should raise a request via ServiceNow.

3.1 User Responsibilities

It is the user's responsibility to:

- Ensure their information on the active directory (global address list) is accurate and up to date. Amendments to account details can be requested via ServiceNow
- Ensure they read, understand, and agree to this policy;
- Report any misuse of council digital communication tools. Please see the Report an information security incident Staffnet pages for more information;

Agree with their line manager the method for return of council equipment when moving role or leaving the council.

3.2 Manager Responsibilities

In addition to complying with their responsibilities as a user, managers are also responsible for ensuring;

- staff they are responsible for understand the standards of behaviour expected of them, and action is taken if behaviour falls below these;
- the correct requests are raised via ServiceNow and/or SAP in a timely manner to protect the council's data and ICT environment. This includes, but is not limited to joiners, movers, or leavers forms, and changes to the active directory (global address list);
- the correct level of permissions are assigned to joiners and/or permissions are revoked when an employee moves to another role, or leaves the council;
- data held within email mailboxes is reviewed and handled in accordance with the Retention Schedule, prior to an employee moving to another role, or leaving the council;

- all corporate assets (laptops, mobile phones etc.) are retrieved, and returned promptly to the Digital & ICT Service when an employee leaves the council, ensuring all possible routes of recovery are explored, as detailed in the Procedure for the return of council ICT equipment.
- any service user/customer information has been added to the relevant case management systems and is not stored within mailboxes and/or on mobile devices.
- all relevant device records/contracts are updated when a member of staff leaves.

4.0 Joiner, Mover and Leaver ICT Requests

Requests will not be completed until the Digital & ICT Service has received the appropriate authorisation(s).

4.1 Joiners

All requests for a new council ICT account must be raised via the joiners form on ServiceNow. This can be found by typing 'joiner' in the search box.

Things to consider when completing a joiner's request:

- If access to an application that is not managed by the Digital & ICT Service is required, a separate request must be raised with the application's asset owner.
- The line manager for the joiner is responsible for assigning any required access permissions.
- Managers are responsible for ensuring that new user accounts and associated permissions are requested at least 10 working days before commencement of employment.

4.2 Movers

If a council employee is moving to a role that requires changes to permission levels, the receiving manager must submit a mover notification via ServiceNow. This can be found by typing 'mover' in the search box.

Things to consider when completing movers requests:

- All movers will be treated as a joiner, with the exception of their email address;
- The Digital & ICT Service will **not** provide a new email address, so any historical emails will not be deleted.
- If access to an application not managed by the Digital & ICT Service is required, a separate request must be raised with the application's asset owner.

For exceptions to any of the above please contact the Digital & ICT Service.

4.3 Leavers

Things to consider when completing leavers requests:

- Requests to remove the access of leavers who do not appear on SAP should be submitted using the non-SAP leaver form available on ServiceNow
- Standard Leaver requests must be raised via the automated process on SAP
- The leaver's data (e-mail and OneDrive) will be accessible for a maximum of 30 days after their account is disabled, to allow their manager to retrieve any relevant information. After the 30 days the account deletion process will take place, there are no exceptions to this due to licensing agreements with Microsoft.
- Removal of access to an application that is not managed by the Digital & ICT Service must be raised as a separate request with the application's asset owner/manager.
- All ICT equipment should be returned to ICT within 30 days.

In line with the Bring Your Own Device (BYOD) policy, if a member of staff has activated BYOD on their personal device to connect to GCC data and systems, all access will be removed when they leave the council's employment.

Further information or advice is available on ServiceNow.

4.4 Account Extension Requests

If an account has not been used for over 30 days, it will be automatically disabled to protect the corporate network and data integrity. In exceptional circumstances (including staff who are on long term sick or maternity leave) an Account Extension request can be raised via ServiceNow with a supporting business case.

Please note: If an account has been fully processed as a leaver (usually after 90 days of inactivity), managers must complete a Joiners form via ServiceNow, instead of an account extension request. The Digital & ICT Service will reject any requests they receive that are raised incorrectly.

5.0 Related policies

- Code of Conduct for Employees
- ICT Equipment Policy
- Information Protection and Handling Standards
- Information/IT Access Policy
- Data Protection Policy
- Software Management Policy

- Social Media Policy
- Password Policy

The above policies are available on Staffnet, or the Information Management and Security Policies pages.

6.0 Policy Compliance

All users with access to the council's data and/or digital communications tools have a responsibility to comply with this policy. Any suspected or observed security breach should be promptly reported to Information Security; further details are provided on the Report an information security incident Staffnet pages.

Where there is a suspected breach of the law, or any council policy (including but not limited to the council's Information Management and Security policies) users should have no expectation of privacy regarding their use of any digital communication tools.

Security breaches by a council employee, 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 information 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.

7.0 Document Control

7.1 Document information

Owner:	Assistant Director: Digital & ICT
Author:	IMS/ICT Policy Group
Reviewer:	Pete Moore, Information Security Adviser
Board(s) consulted:	
Date created:	March 2023
Next review date:	March 2026
Approval:	Information Board

Date of approval:	
Scheme of Delegation ref:	
Version:	1.2
Classification:	UNCLASSIFIED

7.2 Version History

Version	Version date	Summary of Changes
1.0	March 2023	First version. Approved by Information Board on 30.3.23
1.1	August 2023	Minor change to user responsibilities
1.2	April 2025	Broken links fixed and document control table edited

7.3 Review

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

7.4 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