information management & security

Gloucestershire COUNTY COUNCIL

Password Policy

1.0 Policy Statement

Gloucestershire County Council (the council) accepts that information is a valuable asset and must be managed with care. This policy will ensure that users are using suitable authentication methods, such as passwords, and understand their responsibilities to safeguard any information the council holds.

It is a requirement that all users read and accept this policy.

The council will:

- Enforce a number of valid methods to authenticate users including biometrics (fingerprint and facial recognition), strong passwords and passcodes
- Have a standard for the creation of strong passwords
- Determine the frequency of password change across all systems throughout the council
- Ensure that users are made aware of how to use information systems securely
- Check the strength of passwords through auditing and/or automated techniques
- Monitor systems and networks to identify and address network passwords that are suspected or confirmed as compromised

2.0 Risk Management

The council recognises that there are risks associated with use of and access to information and/or information systems.

This policy aims to ensure appropriate access to, and use of, the council's information and information systems, 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

3.0 Scope

This policy applies to all employees, partners, contractors, councillors, agents of the council and other third parties ('users') who require any form of access to the council's information and/or information systems.
All users are expected to comply with this policy at all times when accessing information and/or information systems, whether locally or remotely (e.g. via the Council's Remote Access Gateway, or via any council owned device) or when using systems hosted by authorised third parties. Breach of this policy may result in users being dealt with under the council's Disciplinary and Dismissals Procedure and/or third-party sanctions. Questions regarding the content or application of this policy should be directed in the first instance to the Information Management Service at informationsecurity@gloucestershire.gov.uk.

4.0 Responsibilities

The Council's Assistant Director of Digital & ICT has overall responsibility for the effective operation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to the council's operations lies with Information Asset Owners.

The council's Digital and ICT Service and individual system administrators will provide users with login credentials; users are responsible for changing their password on first log in and ensuring that these are only known to and used by them

Users must not attempt to disable, defeat, or circumvent any council security.

All managers have a responsibility to operate within the boundaries of this policy, ensuring all users understand the standards of behaviour expected of them, and to take necessary action when behaviour falls below these requirements.

It is the user's responsibility to:

- Ensure they read, understand and agree to this policy.
- Use the council's information and information systems in accordance with the terms of this policy.
- Use the council's information and information systems responsibly and in a way that will not harm the council's reputation.
- Ensure they always remember their device passcode/password and their MS365 credentials.
  Users are encouraged to activate biometric authentication for ease of access and improved security where available, but in doing so should be aware that this constitutes explicit consent to the use of their biometrics, as outlined in the NCSC Mobile Device Guidance. Built-in device biometric authentication

features process and capture data entirely on the device itself, and as such will not be collected, stored or attributed to specific users by the council.

- Store application passwords securely using the council's approved password manager solution.

4.1 Things You Must Do

When using the council's information or accessing information systems you **must**:

- ✓ Ensure that your password is not divulged or shared with anyone else.
- ✓ Ensure your passwords adhere to the council's latest Password Construction requirements, on the Staffnet Passwords page.
- ✓ Change your passwords on first log in and in line with this policy.
- ✓ Change your password immediately if you believe your password(s) may have been compromised or if asked to by the DICT service.
- ✓ Create different passwords for your various GCC accounts
- ✓ Where available, configure self-service password reset tools to enable the resetting of forgotten passwords.
- ✓ Always follow the council's best practice guidelines regarding password/passcode complexity regardless of what different applications may enforce
- ✓ Contact the Information Management Service immediately if you become aware of inappropriate access to information or information systems
- ✓ Only access information or information systems when you have a business need to do so.
- ✓ Report any misuse of the council's information or information systems. For guidance on the council's information security incident reporting process please see the Information security incident or concern - what should you do? pages on Staffnet.

4.2 Things You Must NOT Do

When using the council's information or information systems you must **NOT**:

- ✘ Write down and store passwords anywhere except for in the council's approved password manager solution.
- ✘ Reveal passwords over the phone.
- ✘ Reveal passwords on questionnaires or security forms
- ✘ Hint at the format of a password (for example "my family name")
- ✘ Use existing personal account passwords for any GCC accounts (e.g., personal internet (ISP) accounts, banks, etc.) or vice versa.
- ✘ Insert passwords into email messages. (Systems-generated temporary passwords are an exception and **must** be changed as soon as possible in line with the council's password construction requirements on Staffnet)

5.0 Related policies

- Code of Conduct for Employees.
- Information Protection and Handling Policy
- Information/IT Access Policy
- Data Protection Policy
- Software Management Policy
- Information Management Standards for Contractors 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 Information security incident or concern - what should you do? 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.

If you don't understand the implications of this policy or how it applies to you please contact the Information Management Service at informationsecurity@gloucestershire.gov.uk in the first instance.

7.0 Document Control

7.1 Document information

Owner:	Sherrill Holder, Assistant Director of Digital and ICT
Author:	John Deane, Head of Infrastructure and Cyber Security
Reviewer:	IMS/ICT Policy group
Board(s) consulted:	
Date created:	July 2017
Next review date:	January 2027
Approval:	Information Board, May 2021 (v3.0)
Date of approval:	
Scheme of Delegation ref:	
Version:	4.1
Classification:	UNCLASSIFIED

7.2 Version History

Version	Version date	Summary of Changes
0.1	December 2016	Initial document written by The ICT Service
1.0	July 2017	Final version 1 published to Staffnet. Approved by ICT Governance Board July 2017.
2.0	April 2021	Full review of policy by IMS/ICT Policy group. Approved by Information Board May 2021.
2.1	October 2021	Minor revision for accessibility purposes
3.0	May 2023	Full review of policy by IMS/ICT Policy group. Minor change to responsibilities for IAO's, - was not finalised.
3.0	April 2024	Full review completed by IMS/ICT Policy group, broken links fixed.
4.0	June 2025	Review by IMS/ICT Policy group to bring in line with new technology
4.1	January 2026	Review by IMS/ICT Policy group, broken links fixed and related policies section updated.

7.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months in line with PCIDSS requirements.

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