Gloucestershire County Council
Password Policy

1. 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 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

2. 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. Scope

This policy applies to all employees, partners, contractors, Members, 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 3rd parties. Breach of this policy may result in users being dealt with under the council's Disciplinary and Dismissals Procedure and/or 3rd 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. Responsibilities

The Council's Director of Digital & People Services 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 the Assistant Director for Digital & ICT.

The council's ICT Service and individual system administrators will provide users with login credentials; users are responsible for 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 passcode/password.
  Users can choose to activate facial or finger-print recognition for ease of access 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.

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 Password Construction requirements please follow the guidelines available on the Staffnet Passwords page.
- ✓ Change your passwords in line with this policy.
- ✓ Change your password immediately if you believe your password(s) may have been compromised.
- ✓ Create different passwords for your various GCC accounts
- ✓ Be aware that different applications may enforce varying password complexity
- ✓ 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 reporting/investigating a security breach.

Things You Must NOT Do

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

- ✗ Write down and store passwords within the office i.e. in office diaries or paper files.
- ✗ 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 regarded as an exception and can be emailed as these are classified as temporary passwords and **must** be changed as soon as possible)

5. Related policies

- Code of Conduct for Employees.
- Information Protection and Handling Policy
- Information/IT Access Policy
- Data Protection Policy
- Software Management Policy
- Information Security and Handling (Supplier Requirements) Policy

The above policies are available at Information Management and Security Policies

6. 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 its 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

References

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

Policy Review

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

Document Control

Author:	John Deane: Head of Strategy and Architecture
Owner:	Mandy Quayle: Director of Digital & People Services
Document Number:	v2.0

Revision History

Revision date	**Summary of Changes**	**Version**
Dec 2016	Initial document written by The ICT Service	V0.1
July 2017	Final version 1 published to Staffnet	V1.0
April 2021	Full review of policy by IMS/ICT Policy group	V2.0
October 2021	Minor revision for accessibility purposes	v2.1

Document Approvals

Version	**Approved By**	**Date**
V1.0	ICT Governance Board	July 2017
V2.0	Information Board	May 2021
V2.1	N/A	N/A