Gloucestershire County Council
Information/IT Access Control Policy

(Covers: Pre-employment verification checks, information security awareness and training, how access to information and information systems must be controlled, and who is responsible.)

1. Policy Statement

Gloucestershire County Council (the council) accepts that information is a valuable asset and must be managed with care. This policy will set out how access to information and information processing facilities should be controlled, and aims to ensure that users are suitable for their role, and understand their responsibilities. **It is a requirement that all users read and accept this policy.**

2. Risk Management

The council recognises that there are risks associated when using information and accessing IT equipment.

This policy aims to ensure appropriate use and access of information held by the council 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 access to the council's information
- Theft, fraud or misuse of information
- Viruses and other malicious software
- Service disruption

3. Scope

This policy applies to all employees, partners, contractors, agents of the council and other third parties (users) who require any form of access to the council's information (whether in paper or electronic form) and information systems.

This policy should be adhered to at all times when accessing information in any form and from any device. Questions regarding the content or application of this policy should be directed to informationsecurity@gloucestershire.gov.uk.

4. Applying this policy

The council will:

- Put in place pre-employment verification checks that must be undertaken before individuals are authorised to access the council's information systems.
- Put in place processes to ensure user access to information systems is controlled, properly authorised, and promptly removed when the need for access ends.

Ensure that users are trained to use information systems securely.

Recruitment

All recruitment must be undertaken in accordance with the council's recruitment processes and standards. These embody the Government's Baseline Personnel Security Standard (guidelines for the effective screening of personnel). Recruitment checks must be applied to all potential employees, and to all others (e.g. technical support and temporary staff) that have access to the council's information systems or any copies of the contents of those information systems (e.g. backup tapes, printouts, test data-sets).

Security Awareness and Training

All users must receive appropriate information security awareness training and regular updates on legislation and council policies and procedures relevant to their role (users' first point of contact is their line manager). Throughout their period of access to information or information systems users must be trained and equipped to use systems securely.

Access to Information Systems by contractors and third parties

Access to information systems must be controlled in accordance with the Council's Information Security & Handling Standards for Contractors policy

Information systems must have appropriate user access profiles to limit users' access to information based on their role, access must (as far as is practical) be the minimum needed for the users' role, and must be regularly reviewed to ensure it remains appropriate. To ensure the continuing security of information and information systems, users' access to the council's information (i.e. both electronic and manual) must be properly authorised and promptly removed when no longer needed due to change of role or termination of employment (e.g. resignation, suspension, or the end of a contract or project).

Unique user ids and passwords must be used that enable users to be linked to and held responsible for their actions. Use of group/generic user ids must only be permitted where they are necessary for business or operational reasons, these must be documented and where necessary additional controls implemented to maintain accountability.

Passwords must be issued to users in a secure manner, and procedures should be established to verify user identity before providing a new, replacement, or temporary password.

Authentication of External Connections

Remote access to the council's information must be secured by two factor authentication, consisting of a username and password, and a code either via a token, text or a mobile application. Further information is available through the ICT Service. External access to the council's information for staff, partners, contractors, agents or other third parties must be via the council's Remote Access Gateway (Netscaler). Where there is a business need for remote access, applications should be made through the ICT Service Now portal. Additional requirements that apply when working remotely are covered by the ICT Equipment Policy.

Where partners, contractors, agents or other third parties are allowed access to council information then all the considerations of the council's Information Security policies (which can be found at Information Management and Security Policies) apply to them.

5. Responsibilities

HR Responsibility

HR is responsible for ensuring that the recruitment checks required by legislation and statutory bodies are incorporated into the council's recruitment and selection process for all potential employees. HR will review recruitment checks with relevant service areas to ensure this is maintained and updated.

User responsibility

All users are bound by the council's Code of Conduct for Employees to maintain the confidentiality of the information they access; and must not use the information for unauthorised purposes.

Users must:

- Take time to read and understand the council's information security policies which can be found Information Management and Security Policies , and adhere to these policies at all times.
- Undertake and apply information security training made available to them.
- Access personal or special category (sensitive) information only on a need to know basis i.e. they must access only those records necessary to undertake their work. Accessing other records or accounts for any other purpose may be dealt with under the council's Performance Management Capability Procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.
- Follow good security practices in the selection and use of passwords (see the Passwords guidance on Staffnet for more information), and ensure that their password is only known to and used by them. Any user that suspects their password has been compromised must report the incident to the ICT Service Desk and change all passwords in line with the Password Construction guidelines.
- Leave nothing on display and secure anything that may contain access information such as user id's, or tokens.
- Ensure that when allowing other authorised users/third parties access to their desktop/IT equipment, they do not allow them access to information and systems they are not entitled to view e.g. when using webinars, Jabber or service desk facilities
- Ensure that any PC or other device they are using is locked or logged out when left unattended.
- Ensure that paper documents containing personal or special category (sensitive) information are stored securely in line with the council's Information Protection and Handling Standards.
- Return all information and/or information assets when their employment or contract terminates, and ensure that files and documents (including business information on their P drive or email account) are deleted, archived or transferred to another employee in line with retention schedules requirements and any local agreements that exist. Guidance on Good management of your P drive can be found on Staffnet.
- Report any known or suspected breach of this policy. Details of how to report a breach of the Employee Code of Conduct can be found by clicking on the following link Code of Conduct breaches.

- Remote workers shall ensure that the data and systems under their control within their home environment are adequately secured against misuse, loss, theft, and/or damage.

Manager's Responsibility

All managers have a specific responsibility to operate within the boundaries of this policy; to ensure that all users understand their responsibility for information security; and to take action when behaviour falls below requirements.

Managers must ensure that:

- Potential users are recruited in line with the council's recruitment processes which are provided on the HR Recruitment Staffnet page and that pre-employment verification checks (recruitment checks) are undertaken.
- Users are aware of their information security responsibilities and liabilities, and that they must follow the council's information security policies in the course of their work.
- Users are adequately trained and equipped to carry out their role efficiently and securely.
- Information security communications are effectively cascaded to all staff, partners, contractors, agents and other third parties.
- Information security requirements are specified in partnership agreements and third party contracts, see the Information management and security in contracts page on Staffnet.
- New users, role changes, and leavers are promptly processed in accordance with the procedure for corporate systems on the SAP e-form's manager's checklist, and any local process implemented by Information Asset Owners.
- They authorise access to information/IT systems that restricts the users' access to the minimum needed to carry out their role, and regularly review access to ensure it remains appropriate.
- The ICT Service Desk is promptly notified of an employee's suspension so that their network access (including remote access) can be disabled.
- Users return all of the council's assets in their possession upon termination of their employment, contract or agreement (including information in any format e.g. electronic or paper, and devices such as laptops, mobile phones and tablets).

Information Asset Owners Responsibility

Information Asset Owners are responsible for putting in place formal procedures to control the allocation of access rights to information and systems. This should include:

- Understanding and addressing risks to the information asset, and ensuring appropriate security measures are in place to protect the information, based on the content and impact of disclosure.
- Designing and implementing appropriate user access profiles for information systems using standard profiles for common jobs (e.g. system administrator, manager, clerk, social worker etc.), designed to ensure that as far as possible users' access to information is limited to that needed for their role.
- Designing and implementing a process for user registration and management that requires line management authorisation for user access to information and IT systems, and includes using unique user id's and passwords to ensure that users are linked to and accountable for their actions.
- Ensuring that the use of privileged accounts (such as system administrator accounts) is restricted to users who are required to perform such tasks, and is tightly controlled.
- Putting in place processes to ensure that access to information systems remains appropriate for the users' role, and facilitating changes in respect of new users, role changes, and employment termination or suspension.
- Ensuring system users receive appropriate training to enable them to protect information and use the system securely.
- Ensuring that reported security incidents or concerns are investigated, addressed and appropriate action taken to prevent reoccurrence.
- Ensuring that systems are configured in accordance with the Information Security & Handling Standards for Contractors policy

Help and Guidance for Information Asset Owners and access to the Information Asset Register is available on Staffnet at: Information Asset Owners

ICT Responsibility

ICT will:

- Provide technical security advice and support
- Develop relevant policies, procedures and guidelines in conjunction with the Information Management Service
- Implement and administer appropriate technical security controls
- Maintain accreditation with PSN and Cyber Essentials Plus

- Maintain evidence of data protection compliance by carrying out system audit exercises and ensuring the system access policy is adhered to via a system access form for all new users.

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; further details are provided at Information security incident or concern - what should you do?.

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 its reasonable opinion such a 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 following for advice: Information Management Service on 01452 42(5812) or informationsecurity@gloucestershire.gov.uk.

7. References

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

8. Policy Review

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

Document Control

Author:	Sue Blundell, Corporate Information Security Advisor
Owner:	Rob Ayliffe, Director of Policy, Performance and Governance. (Chief Information Officer and Senior Information Risk Owner)
Approval body/date	Information Board
Document Number:	v2.1

Revision History

Revision date	**Summary of Changes**	**Changes marked**
May 2018	Updated links due to new IMS pages on staffnet and changed review period to 3 years. Also added references to webinars.	1.5
June 2020	Minor revisions to update links and bring the policy in line with standard policy format	2.0
October 2021	Minor changes for accessibility purposes including change of policy owner and review of hyperlinks.	2.1

Approval History

Version	Approval Body	Date
1.0	Information Board	24/10/11
1.1	Information Board	19/12/2012
1.2	Information Board	16/10/2014
1.3	No approval required; updated hyperlinks only	N/A
1.4	No approval required; updated hyperlinks only	16/12/2016
2.0	Information Board	19/06/2020
2.1	No approval required; updated hyperlinks only	N/A