information management & security

Gloucestershire COUNTY COUNCIL

Remote Working (Information Management & Security) Policy

1.0 Policy Statement

The purpose of this policy is to protect Gloucestershire County Council (the council), its information and data, assets, employees and service users from the consequences of accidental loss or disclosure of personal and special category (sensitive) information. In this context, the policy sets out the council's authorised methods for managing information when working remotely.

The council provides employees with the equipment, facilities and opportunities to work in an agile way both remotely as well as at council premises (whilst also recognising that there may be some roles for which remote working is not suitable).

2.0 Risk Management

Working remotely away from council premises creates additional risks with respect to information management and security; for both hard copy information and for data stored electronically. Employees and other users are responsible for ensuring that these risks are recognised and minimised in line with data protection and related legislation and best practice.

Employees and other users must recognise that they may be held liable under the law and council policy, where a data breach occurs.

When working remotely information in any format, whether paper or electronic, and all ICT equipment used for remote access to the council's information systems, **must** be managed effectively to minimise the risk of unauthorised access, disclosure, or loss of personal or special category (sensitive) information that could result in:

- Harm to service users or employees
- Service disruption
- Potential legal action and/or fines against the council or employee
- Damage to the council's reputation
- Theft, fraud or misuse of facilities

3.0 Scope

This policy applies to all councillors, employees, partners, contractors, agents of the council, GFRS and other third parties (users) who use the council's ICT facilities and equipment remotely, or who require remote access to the council's information, or information systems.

4.0 Related Policies

This policy should be read in conjunction with the following policies which can be found on the council's information management and security policies webpage.

- Special Category Data Policy
- Information Security Incident Management Policy
- Information Security Policy
- Information/IT Access Policy
- Information Protection and Handling Standards
- Code of Conduct for employees

5.0 ICT Equipment

Equipment such as laptops, tablets and mobile phones are provided for employees to conduct council business. These devices, and any information temporarily stored on them, are a valuable asset and also constitute a risk to information management and security.

A council-managed device is defined as being subject to centralised security controls, processes and procedures managed by D&ICT. Council-managed devices will be subject to regular patch and antivirus updates.

A BYOD device is defined as an employee's personally owned device(s) used for work purposes. Staff must ensure that any BYOD devices are subject to regular patching and anti-virus updates. These must be used in accordance with our Bring Your Own Device (BYOD) policy.

When using **any** ICT equipment to access council systems and data you must safeguard the device(s) and data appropriately, and in line with the council's information management and security policies, whether on council premises or at another location.

Employees can safely use public WiFi to access the council's Microsoft tenancy as the associated Virtual Private Network (VPN) enables the encryption of data over a secure connection. Those systems that have single sign on or are accessed via the GCC network can also be accessed securely in the same way. To confirm whether or not third-party systems accessed via an alternative route have the same level of protection when using public WiFi, please raise a ticket on ServiceNow.

6.0 Device Security

- All devices used to access council systems and data must receive regular operating system (e.g. Windows) and security updates.
- For council-managed laptops to receive their updates, they must be connected to the corporate network where possible on a weekly basis to ensure patches are applied as soon as they are released and as a minimum on a monthly basis to ensure they are maintained, and all windows and security updates are installed. Updates will be applied automatically when logging in at council premises, for example in Shire Hall.
- Authentication information (e.g. access tokens and/or passwords) must not be stored with laptops, tablets and mobile phones, either in transit or at home. Passwords must never be written down or shared.
- Council-managed devices must be logged off and shut down when not in use, or locked when away from your desk/taking a break Staff using BYOD devices must ensure all council systems are logged off when not in use or if the BYOD device is left unattended.
- When transporting council-managed laptops this must be done in a suitable padded carry bag (preferably unbranded) or strong briefcase to reduce the chance of accidental damage.
- Council-managed devices must be returned to D&ICT on request, to facilitate software and/or hardware audits or enable security/maintenance work, and at the end of a user's employment/assignment, as appropriate.

7.0 Information

- The confidentiality of personal or special category (sensitive) information, whether held on paper or electronic media (including the data displayed on screen), must be safeguarded from unauthorised access or disclosure at all times, whether working in transit (e.g. on a train), at home, or any other remote location.
- Under no circumstances should personal or special category (sensitive) information be either sent to a user's personal or home email account or transferred to removable media (including a safe stick) for the purposes of remote working using a BYOD device.
- A council-managed device may be used as a standalone device where access to the network is not available. Council information that is temporarily stored on the device must be regularly saved to the appropriate system to ensure the ongoing availability of that information in case of device corruption, failure or theft. Personal or special category (sensitive) information relating to individuals in receipt of support/services from the council must be added to their individual record (e.g. on LiquidLogic) in a timely manner, preferably on the same day but no later than 3 calendar days after the event.
- Personal or special category (sensitive) information must be secured when being transported. This is best achieved by using a council-managed device.
- Emails must be encrypted as appropriate. Please see the guidance on Secure Email.
- Personal and/or sensitive documents must be stored securely and in accordance with the council's Information Protection and Handling Standards.

- Prevent the loss of hard copy information by only using and storing it safely on council premises. Where hard copy information needs to be retained in line with the council's retention policy but doesn't need to be accessed on a regular basis, it should be deposited with the Records Centre.
- In circumstances where information in paper form must be taken outside council premises, the additional risks associated with this and the need to ensure the information is protected must be addressed beforehand.
- Documents must only be printed where it is essential to do so. When working in council premises, staff must use corporately provided printing facilities.
- When printing multiple copies of any document, staff must ensure they collect all copies; not doing so will result in an information security breach.
- Staff needing to send correspondence to members or the public and/or external bodies should make use of DocMail (print to post), which allows the printing and posting of documents directly from their desktop.
- All personal or special category (sensitive) information must be disposed of using the council's confidential waste facilities. It can be shredded using a personal shredder; but the resulting shreds must then be disposed of using the council's confidential waste facilities.

8.0 Environment

The environment in which users are working must always be considered and reasonable steps taken to prevent or reduce the possibility of damage, loss, or theft of council managed devices or data.

Information must be protected from prying eyes and ears when working in public places.

- Family members, friends, or visitors must not use council-managed devices or access council information. If BYOD devices are shared across a family, users must log out of all council systems at the end of every session and must not save passwords to device-specific password managers.
- Devices and/or documents must be secured when unattended e.g.
    a. In your home – close or lock windows and keep equipment and documents out of sight.
    b. Don't leave devices or documents containing personal or sensitive information in your vehicle. In exceptional circumstances where you have no alternative, ensure that they are in the boot out of sight and the vehicle locked. Remember you must use sound judgement and be able to account for your actions if challenged.
    c. Never leave a laptop, tablet, mobile phone, or documents in your vehicle overnight (note - if the device is covered by the council's 'all risks' insurance policy leaving it in an unattended vehicle invalidates this insurance).
    d. Never leave a laptop, tablet, mobile phone or documents unattended in a public place e.g. train or café.
    e. ICT equipment must be locked when leaving it unattended at work or home, even for a very short period of time..

9.0 Responsibilities

9.1 Managers' Responsibilities

Managers must ensure that the risks associated with remote working are adequately addressed.

Managers must ensure that:

- Employees and other users are aware of their responsibilities under this policy, the Data Protection Act 2018, and other Information Management and Security Policies.
- Proposed working arrangements provide adequate security to safeguard personal or special category (sensitive) information, comply with the council's Information Management and Security policies, and fulfil the council's responsibilities under the Data Protection Act.

9.2 Users' Responsibilities

Users must ensure that:

- They are familiar with, and adhere to the content of this, and related Information Management & Security policies before working remotely.
- They treat council-managed devices with respect; they are both expensive and can be fragile and easily damaged. Carry and store them in an appropriate protective case and take care when eating and drinking whilst working.
- They use council-managed devices only for the purpose for which they were issued, and in accordance with the council's ICT Equipment Policy, and any device-specific acceptable use policy and/or operating instructions provided.
- They take account of the environment in which they are working and take reasonable care to prevent or reduce the possibility of damage, loss, or theft of council equipment or information.
- In circumstances where they must take information in paper form, they consider the additional risks and how they will protect the information in transit.
- They report the loss or unauthorised disclosure of personal or special category (sensitive) information to their line manager and in accordance with the council's incident reporting procedure as soon as they become aware of it.
- They report all technical faults, accidental damage, or queries to ServiceNow.
- They report the theft of any council device to the Police, ServiceNow, the Information Management Service and their line manager as soon as they become aware of it.
- They report the theft of any BYOD device to ServiceNow, the Information Management Service and their line manager as soon as they become aware of it.
- They understand that unauthorised disclosure of personal or special category information due to negligence on their part could make them liable to prosecution under Data Protection legislation.
- Ensure that they have no restrictions on home working (failure to inform domestic insurers may result in home insurance cover being rendered invalid).

10.0 International Remote Working

In order for a user to access council systems and information outside of the UK the council must comply with Article 5 of the UK GDPR and the Information Commissioner's guidance on international transfers.

This means that the country must have an adequacy agreement with the UK, or that there are appropriate safeguards in place to protect personal data being accessed in that country. Alternatively, consent to the processing would have to be sought from any data subject whose personal data may be processed by the user in that country. There are no suitable appropriate safeguards applicable to the council and obtaining consent from all data subjects prior to working remotely would be impractical and extremely unlikely. As such, the council only allows automatic access to systems and information where a user is based within the;

- UK,
- European Economic Area (EEA),
- Gibraltar, Guernsey, Isle of Man, Jersey, and Switzerland, and
- Countries that have a full adequacy decision (a list is available from the ICO website).

The list of countries from which access can be provided will be regularly monitored and updated by the Information Management Service as and when adequacy agreements with other countries are established.

Please note that access to council systems and personal data by suppliers based outside of the UK is governed by the council's Cyber and Information Management (Procurement) Policy.

11.0 Policy Compliance

All users must comply with this policy, which can be found on the Information Management and Security Policies webpage. If you do not understand the implications of this policy or how it applies to you, seek advice from the Information Management Service at informationsecurity@gloucestershire.gov.uk

Breaches of this policy or any other security policy requirements as a result of deliberate or negligent disregard may be dealt with under the Council's Disciplinary and Dismissals Procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

In the event that information security 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 may take such punitive action against that user and/or their employer as the council in its absolute discretion deems appropriate.

The council has a legal obligation to inform the Information Commissioner of information security breaches in certain circumstances within 72 hours.

The council may, in its absolute discretion refer the matter of any breach of the council's security policy requirements to the police or other regulatory body for investigation and (if appropriate) the instigation of criminal or professionally linked proceedings, if in the reasonable opinion of the council, such a breach has or is likely to lead to the commissioning of a criminal offence or be in breach of professional standards.

12.0 Learning and Development

The council will provide a range of **mandatory** learning and development to ensure that all employees understand their responsibilities with respect to information management and security.

This will include sections in the corporate induction, a specific Information Management and ICT Induction and regular annual refresher events.

Employees will have to undertake this learning to be able to use the council's technology and information.

For more information, please contact informationsecurity@gloucestershire.gov.uk

13.0 Document control

13.1 Document information

Owner:	Director Policy, Performance & Governance (SIRO)
Author:	Jenny Grodzicka, Head of IMS, Dave Morgan, HR Adviser
Reviewer:	IMS & D&ICT Policy Group
Board(s) consulted:	Information Board
Date created:	November 2020
Next review date:	January 2028
Approval:	Rob Ayliffe, Director Policy, Performance & Governance (SIRO)
Date of approval:	
Scheme of Delegation ref:	DPPG1
Version:	2.1
Classification:	UNCLASSIFIED

13.2 Version History

Version	Version date	Summary of Changes
1.1	November 2021	Additional section added on International Remote Working Minor changes for accessibility purposes and review of hyperlinks.
1.2	May 2022	Updated information on Adequacy Agreements and included link ICO guidance.
1.3		Not published.
1.4	October 2024	Broken links amended, document format updated and minor content changes.
2.0	January 2025	Section added on the use of public WiFi. Section added on retention and use of the Corporate Records Centre. Additional guidance added on family use of BYOD devices. Definition of BYOD device added. Definition of council-managed device updated.
2.1	July 2025	Link to ICO webpage updated with regard to international transfers.

13.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years or when there are changes to relevant legislation.

13.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: mailto:dpo@gloucestershire.gov.ukdpo@gloucestershire.gov.uk

Phone: 01452 324000