Gloucestershire County Council
Remote Working (Information Management & Security) Policy

1. 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.

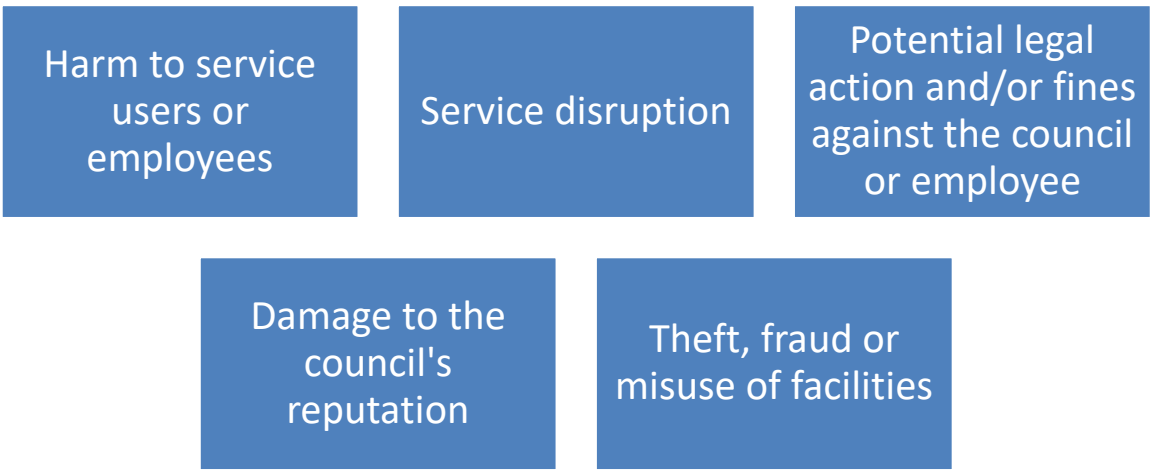
The council provides employees with the equipment, facilities and opportunities to work in an agile way both remotely as well as at council premises (whilst also recognising that there may be some roles for which remote working is not suitable).This acknowledges the progress made with respect to 'new ways of working', the benefits to business need and service delivery, to the climate emergency, the opportunity for an improved work life balance for many of our employees, the most efficient use of our resources, and in response to the Covid-19 pandemic.

2. Risk Management

Working remotely 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:



3. 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. 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.

5. ICT Equipment

Equipment such as laptops, tablets and mobile phones are provided for employees to conduct council business. These devices, and any information 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 provided by ICT. Council managed devices will be subject to regular patch and antivirus updates. When using council ICT equipment, 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.
- use the council's Remote Access Gateway (NetScaler) to access the council's network. It provides remote access to systems and data in a controlled way to minimise risk, using dual-factor authentication (i.e. two means of authenticating a user, such as the number generated by a token and a password).
- access the council's network and personal or special category (sensitive) information via a council owned and managed device. Before allowing a user access, NetScaler will check to ensure the connecting device is authorised, and that software on the connecting device meets the required standards. If the connecting device fails, these tests access will be denied.

The Council's mobile device security solution (Blackberry Work) may (subject to eligibility and conditions for use) be used with a user-owned personal device such as a smart phone or tablet to access council email, contacts, calendar, P Drive and

StaffNet via the device's own data connection or Wi-Fi. This is the councils only approved 'Bring Your Own Device' solution. Further information is available on the ICT Service's Blackberry Work staffnet page.

Employees and workers using Blackberry Work to access council systems and data must safeguard these in line with council policies.

6. Device Security

- Laptops must receive regular windows and security updates. To achieve this, they must be connected to the pink/purple layer at a minimum of a monthly basis to ensure the devices 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 and mobile phones, either in transit or at home. Council ICT passwords must never be written down or shared.
- Devices must be logged off and shut down when not in use - for example when working from home and taking a break, as a minimum the laptop should be locked using *ctrl-alt-delete or Windows & L keys*.
- The configuration of the device must not be changed.
- When transporting devices this must be done in a suitable padded carry bag (preferably unbranded) or strong briefcase to reduce the chance of accidental damage.
- Council devices must be returned to 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. 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 non GCC or home PC/laptop.
- A corporately managed device may be used as a standalone device where access to the network is not needed. Council information that is temporarily stored on the device must be regularly saved to the network to ensure the availability of the information in case of device corruption 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. Liquid Logic/Eric) in a timely manner and no later than 3 working days after the event and preferably on the same day.

- Personal or special category (sensitive) information must be secured when being transported. This is best achieved by using a corporately managed device.
- Emails must be encrypted as appropriate using the Egress functionality. Please see the guidance on Secure Email.
- Personal and/or sensitive documents must be stored securely and in accordance with the council's Information Handling Standards.
- Avoid losing information by using and storing it safely on council premises. If information does need to be taken outside council premises only the specific information needed should be taken (for example don't take a client record file if all that is needed is their name and address).
- 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 should use the Multi-Function Devices (MFD) which allow the collection of printing from any device in any location, or other corporately provided printing facilities where MFDs are not available. The Print Room should be used for large scale or specialist printing.
- When working remotely, staff should make use of DocMail, 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. 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-owned laptops, mobile phones or data.

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

- Family members, friends, or visitors must not use the council's devices or access information**.**
- 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.
    c. Never leave a laptop, mobile phone, or documents in your vehicle overnight (note - if the device is covered by the council's 'all risks'

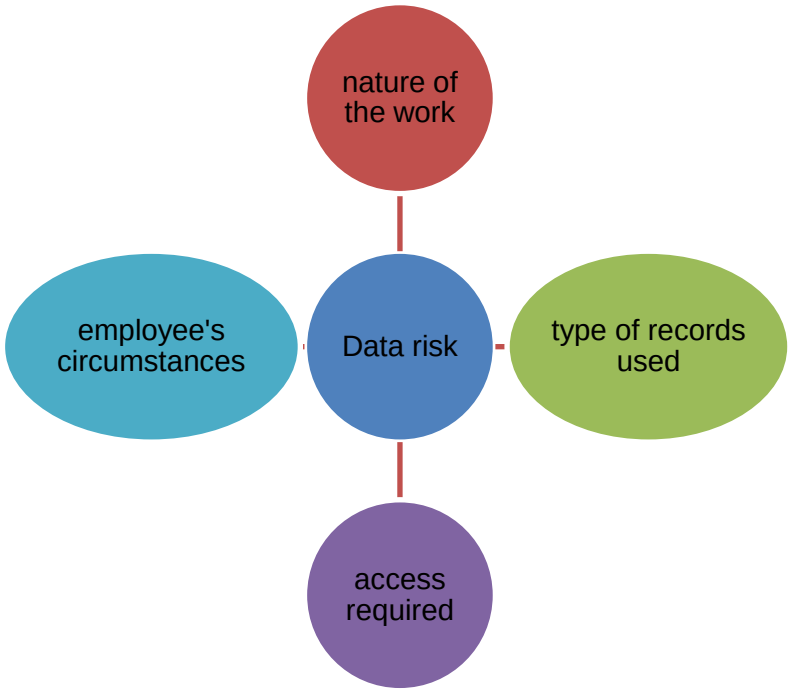
insurance policy leaving it in an unattended vehicle invalidates this insurance).

d. Never leave a laptop, mobile phone or documents unattended in a public place e.g. train or café.
e. ICT equipment must be locked (e.g. using Ctrl, Alt, Delete or Windows & L keys) when leaving it unattended at work or home, even for a very short period of time, for example to make a drink or go to the toilet.

9. Responsibilities

9.1 Managers' Responsibilities

The information and data risks associated with an employee working remotely will depend on:



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 document and related Information Management & Security policies before working remotely.
- They treat council 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 owned laptops and mobile phones only for the purposes for which the council has provided them, and in accordance with the council's ICT Equipment Policy, and 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 devices 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 the ICT Digital Desk.
- They report the theft of any council device to the Police, the ICT Digital Desk, 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. International Remote Working

In order for a user to access council systems and information outside of the UK the council must comply with Chapter 5 of 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. 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. 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. Policy 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.

Document control

Author:	Jenny Grodzicka, Head of IMS and Data Protection Officer Dave Morgan, HR Adviser
Owner:	Rob Ayliffe, Director of Policy, Performance & Governance (Senior Information Risk Owner)
Document Number:	v1.2
Creation Date:	November 2020

Revision date	Summary of Changes	Changes marked
November 2021	Additional section added on International Remote Working Minor changes for accessibility purposes and review of hyperlinks.	1.1
May 2022	Updated information on Adequacy Agreements and included link ICO guidance	1.2

Document Approvals

Version	Approved By	Date
1.0	Information Board	December 2020
1.1	Information Board	November 2021
1.2	N/A	May 2022