Gloucestershire County Council
Internet and Digital Communications Policy

1. Policy Statement

Gloucestershire County Council (the Council) accepts that the internet and digital communications are essential to enabling the Council to meet its aims and objectives. It is a requirement that your use of the Council's internet and digital communications facilities is legal and appropriate for delivering the Council's responsibilities and does not create unnecessary risk. The Council will ensure that users have access to its internet and digital communications facilities. It is a requirement that all users read and accept this policy.

The Council's internet and digital communication facilities are made available to users for Council business purposes. Limited personal use is permitted, provided that such use is strictly in accordance with this policy which can be found at Information Management and Security Policies

2. Risk Management

The Council recognises that there are risks associated with use of the internet and digital communications tools.

This policy aims to ensure appropriate access to, and use of, the Council's internet and digital communications facilities, 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 anyone who uses the Council's internet and digital communications facilities.

Digital communication facilities include, but are not limited to, email, instant messaging apps, video conferencing/calling, webinars, text messaging and telephony.

All internet and digital communications users are expected to comply with this policy at all times when using the Council's internet and digital communication facilities,

whether accessed locally or remotely (e.g. via the Council's Remote Access Gateway; or via any Council owned device). Breach of this policy 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.

4. Responsibilities

The Council's Director: Strategy & Challenge 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 Head of ICT.
If you do not understand the implications of this policy or how it may apply to you, you should seek advice from the ICT Service Desk.

The Council's ICT Service will provide users with a logon id and password for their network account; this also controls access to the internet. Users are responsible for ensuring that any logon id and passwords are only known to and used by them. Users must not attempt to disable, defeat, or circumvent any Council security

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

5. User Responsibility

Use of the internet and digital communication facilities must be consistent with the Council's Code of Conduct for Employees. All users are responsible for using the Council's internet and digital communication facilities appropriately and in accordance with the statements in this policy.

It is the user's responsibility to:

- Ensure they read, understand and agree to this policy as part of their induction to the Council;
- Use the Council's internet and digital communication facilities in accordance with the terms of this policy;
- Use the internet and digital communications responsibly and in a way that will not harm the Council's reputation;
- Recognise that the Council's internet and digital communication facilities are provided for business use and must be protected from unreasonable and excessive personal use;
- Report any misuse of the Council's internet or digital communication facilities. Follow the reporting a security incident link for more information.

6. Related policies

- Code of Conduct for Employees.
- ICT Equipment Policy
- Information Protection and Handling Policy

- Information/IT Access Policy
- Data Protection Policy
- Software Management Policy
- Social Media Policy
- Password Policy

The above policies are available at Information Management and Security Policies

7. Things You Must Do

When using the Council's internet and digital communications facilities you **must**:

a. Security controls and use of your account details, you must:

- ✓ Ensure that your logon id and password is only known to and used by you;
- ✓ Keep your personal use of the internet and digital communication facilities to a minimum;
- ✓ Assess the reliability of any information before using it (e.g. that it is from a reliable source, accurate, complete and current);
- ✓ Comply with the legal protections to data, images, and video provided by copyright and licenses;
- ✓ Inform the ICT Service Desk immediately of any unusual occurrence (e.g. an antivirus software warning, getting pop-ups without having your browser open, unable to open files or task manager)

b. *Access, you must*

- ✓ Contact the ICT Service Desk immediately if you receive a suspected virus or if you experience any unusual occurrences in respect of the Council's digital communication facilities (e.g. an antivirus software warning).

c. Content, you must

- ✓ Take care to ensure that your communications (messages) are sent only to those who should receive them. Re-read messages before sending, check for correct addressing and (particularly where they include personal or special category information), clarity, and ensure that the content will not embarrass or subject the Council to legal proceedings or a fine.
- ✓ Take care to ensure that any calls you make or receive cannot be overheard. You should be fully aware of your environment at all times, and avoid making calls that refer to personal or special category information in public places, over loud-speaker or when using hands-free devices. You should also try to ensure that the recipient of your call takes these same considerations into account.
- ✓ Use Egress to encrypt your communications (messages) when they include personal or special category information and are being sent outside the Council's secure network
- ✓ Put in place arrangements to ensure that incoming messages are dealt with during periods of planned absence.

- ✓ Retain messages which constitute an official record in accordance with the Council's Records retention and disposal schedule
- ✓ Manage the contents of your accounts to retain them within the current maximum limit.
- ✓ Put in place arrangements to ensure that the business content of your account is available to those who need it before you change role or leave the Council's employment.
- ✓ Exercise caution when opening emails and messages from an unknown external source or where, for any reason, they appear suspicious.
- ✓ Inform your line manager if you feel you have been harassed or bullied, or you are offended by material received from a colleague via digital communications. Information and advice on the Council's Whistleblowing policy and procedure can be on the employee information and support intranet pages.

8. Things You Must Not Do

In using the Council's internet and digital communications facilities you must **NOT**:

a. Security controls and use of your account details, do not:

- ✘ Attempt to disable, defeat, or circumvent any Council security mechanism;
- ✘ Send messages from another user's account or under an assumed name unless specifically authorised.
- ✘ Respond to messages requesting personal information such as credit card details, user names or passwords, or containing links to internet sites where such information is requested.
- ✘ Transmit any message or file attachments you know or suspect to be infected with a virus.
- ✘ Subscribe to mailing lists for personal purposes using your Council credentials, such as your email address, except for goods ordered from the Gloucestershire Portal GCC Staff Discounts.

b. Personal, special category and sensitive information, do not:

- ✘ Upload personal or sensitive information into non-contracted systems, unless otherwise authorised, for example when required to provide information by law;
- ✘ Send personal or sensitive information by non-secure means, unless otherwise authorised, for example where the service user is aware of the risks and has requested communication by other means;
- ✘ Forward personal, special category or sensitive information to an external location (including your personal home email address) or to another person who may not be authorised to see the information.

c. Access, do not:

- ✘ Access emails intended for others that are clearly marked 'personal' or addressee only (for example when providing cover for periods of absence).

- ✘ Access systems containing personal, special category or commercial data over Public Wi-Fi;
- ✘ Allow other authorised users/third parties with access to your desktop/IT access to information and systems they are not entitled to view e.g. when using webinars, Jabber or service desk facilities;
- ✘ Allow third parties, contractors or suppliers, other than the current corporate ICT service provider, to remotely access/take over your PC or laptop via the internet (a supplier or contractor can instigate this by for example asking you to accept a connection or click on a link on their website) for advice contact ICT Service Desk.

d. Content, do not:

- ✘ Create, download, upload, display or knowingly access sites that contain, or might be deemed to be:
  - Pornographic
  - Illegal
  - Obscene or offensive (racially, sexually, religious, disability or otherwise discriminatory, or of an extreme political nature)
  - Subversive or violent.
- ✘ Send messages or create or send content that violate the privacy of, or unfairly criticise others or that may damage the Council's reputation, unreasonably waste staff resources, or disrupt the work of other email users.
- ✘ Inadvertently send messages containing statements which are likely to create liability (whether criminal or civil, and whether for you or the Council).
- ✘ Send commercial or advertising material, chain letters, or junk mail (otherwise known as spam) of any kind.
- ✘ Click on links or attachments within emails or messages from unknown or suspicious external sources (for example if the attachment ends in .exe)

e. Copyright, do not:

- ✘ Download any information, distribute or store pirated software, music, or documentation or any material that may be subject to copyright or formally licensed.

f. Subscriptions and contract terms, do not:

- ✘ Subscribe to, enter or use online gaming or betting sites.
- ✘ Subscribe to or enter 'money making' sites or enter or use 'money making' programs.
- ✘ Agree to terms, enter into contractual commitments or make representations unless appropriate authority has been obtained

g. Software, do not;

- ✘ Download any software including but not limited to: software that allows sharing of music, video or image files; screen savers or games.

h. Private use, do not:

- ✘ Use the Council's internet or digital communication facilities to order/purchase goods and services for personal use except via the Gloucestershire portal at GCC Staff Discounts, purchases via the portal **must not** be delivered to Council premises;
- ✘ Personally subscribe to or use: real time chat facilities such as chat rooms, instant messaging, or social networking sites such as Facebook or Twitter with your Council credentials. This excludes authorised use required to deliver Council services (e.g. online digital support and social media engagement)
- ✘ Undertake any private buying, selling or monetary transactions e.g. online trading using sites such as eBay, or personal bank account transactions using Council facilities;
- ✘ Use Council facilities to run a private business.

Use of the Council's internet or digital communication facilities for any of the above purposes (this list is not exhaustive) will amount to gross misconduct. Any such action will be treated very seriously and is likely to result in summary dismissal.

9. Personal Use of the Council's Internet Facilities

At the discretion of the users' line manager, and provided it does not interfere with their work, the Council permits personal use of its internet and digital communication facilities in the users' own time, provided that any use is in accordance with this policy and subject to the conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and the Council reserves the right to withdraw its permission at any time.

The following conditions must be met for personal use to continue:

- Use must be minimal and take place outside of normal working hours (i.e. during lunch hours, before or after recorded working hours);
- Use must not interfere with business or office commitments;
- Use must comply with the Council's information security policies which can be found at Information Management and Security Policies.

Personal messages should be identified by users by inserting the word '*personal*' in the subject heading. Every effort will be made to protect the confidentiality of '*personal'* messages during cover for periods of absence; however, you must be aware that confidentiality cannot be guaranteed.

If users are in any doubt about how they may make personal use of the Council's facilities they should consult their line manager.

10. Privacy information for GCC Mobile Wi-Fi

Gloucestershire County Council is the data controller for personal data collected as part of providing the Mobile Wi-Fi service. The personal data collected is;

- The device name,

- The MAC address of the device connecting to the Wi-Fi, and
- The IP address of the device connecting to the Wi-Fi.

This data is collected and used in order to;

- monitor use of the Wi-Fi facility, including web sites visited. This is part of the Council's responsibility as a provider of an Internet service. This service is provided by Cisco.
- help the Council to understand how our Wi-Fi is used by providing analytical data. For example it can tell us how many people are connected and for how long. This information is very important to us as it enables us to plan how we can improve the service.

Personal data is retained for a maximum of 14 months, although anonymised data may be retained for longer. All personal data will be held within the EEA.

For further information, and how to use your data protection rights, please read the Council's Privacy Notice which can be found at https://www.gloucestershire.gov.uk/privacy

11. Monitoring

Users should be aware that all use of the Council's systems can be monitored, and where breaches of this policy are found, action may be taken under the Council's Disciplinary and Dismissals Procedure.

While all activity may be recorded; monitoring is only carried out to the extent permitted or as required by law, and as necessary and justifiable for the Council's business purposes. The specific content of any correspondence will not be monitored unless there is suspicion of improper use.

Any Council device used and any data processed by users remains the property of the Council and may be accessed at any time by the Council to ensure compliance with its statutory, regulatory, and internal policy requirements.

To monitor whether use of the facilities is in accordance with this policy, to assist in management investigations, to comply with any legal obligation, for capacity management and for security reasons the Council reserves the right to:

- restrict or prevent access to certain facilities or introduce routine monitoring if personal use is considered to be excessive.
- not to transmit any message and/or to block access to attachments for the purpose of efficient and effective use of the system and/or compliance with this policy.
- monitor internet sites visited by users and the volume of internet traffic, and use of digital communication facilities for the following purposes (this list is not exhaustive):

Web traffic filtering software is in place to block or limit access to inappropriate sites from the Council's data network. Blocked sites may be made available to individual

internet users or groups of internet users where there are sound business reasons for doing so, and following a risk assessment and approval by the appropriate line manager. To apply for access to a blocked site contact the ICT Service Desk.

The filtering system records all internet activity; there is no distinction between business and personal use. The information recorded includes but is not limited to the user's name, the date & time and the site accessed. These records are retained for up to six months.

A fully automated process is in place for checking incoming emails for viruses and spam/junk email. Emails that are regarded as spam/junk email will be automatically deleted. Emails identified as potential spam are quarantined, and brought to the email user's attention via the Personal Email Manager. This process is fully automated with no human intervention.

If a manager or investigating officer believes that internet or digital communication facilities have been misused, spot checks and/or reports may be produced to support investigations. To obtain activity reports contact the ICT Service Desk.

When a website is visited, technologies such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in point 12 such a marker could be a source of embarrassment to the visitor and the Council, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

12. Policy Compliance

Anyone with access to the Council's internet or digital communications facilities has 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 on the Reporting/investigating a security breach site.

Use of the Council's internet or digital communication facilities for any of the prohibited purposes in this policy (this list is not exhaustive) will amount to gross misconduct. Any such action will be treated very seriously and is likely to result in summary dismissal.

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 internet activity or use of digital communication facilities.

Where evidence of misuse is found to have taken place a more detailed investigation may be undertaken in accordance with the Information Security Incident Response and Escalation Procedure, involving the examination and disclosure of monitoring

records to those nominated to undertake the investigation and any witnesses or manager(s) involved in this procedure.

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.

13. References

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

14. Policy Review

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

15. Document Control

Author:	Peter Moore: Information Management Service
Owner:	Jane Burns, Director: Strategy & Challenge (Chief Information Officer and Senior Information Risk Owner)
Document Number:	V2.4

Revision date	**Summary of Changes**	**Changes marked**
October 2018		V2.0
March 2019	Review of section 8 – 'Things you must not do'	V2.1
January 2020	Inclusion of privacy information for the GCC Mobile Wi-Fi service	V2.2
April 2020	Added guidance on awareness of environment when making phone calls	V2.3
December 2020	Reviewed and updated hyperlinks	V2.4

16. Document Approvals

Version	Approved By	Date
V2.0	Information Board	December 2018
V2.1		
V2.3		
V2.4		