Gloucestershire County Council
Cisco Jabber Acceptable Use Policy

1. Policy Statement

Gloucestershire County Council (the council) accepts that the use of collaborative software (Cisco Jabber) is essential to enabling the council to meet its aims and objectives. It is a requirement that your use of this software 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 this software.

Cisco Jabber is made available to users for council business purposes only.

2. Risk Management

The council recognises that there are risks associated with the use of collaborative tools.

This policy aims to ensure appropriate access to, and use of, collaborative software, which will in turn 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 collaborative software.

Collaborative software includes, but is not limited to, the ability to divert desk phones to mobile devices, share desktops, facilitate conference calls and use instant messaging.

All Cisco Jabber users are expected to comply with this policy at all times when using the council's collaborative software, 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 of People 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.

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 Cisco Jabber must be consistent with the council's Code of Conduct for Employees. All users are responsible for using the council's collaborative software appropriately and in accordance with the statements in this policy.

It is the user's responsibility to:

- Ensure they read and understand this policy;
- Use the council's collaborative software in accordance with the terms of this policy;
- Use Cisco Jabber responsibly and in a way that will not harm the council's reputation;
- Recognise that the council's collaborative software is provided for business use and must be protected from unreasonable and excessive personal use;
- Report any misuse of Cisco Jabber. Details of how to do this are provided on the Reporting and investigating a security breach Staffnet page

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 Cisco Jabber you **must**:

- ✓ Ensure that your logon id and password is only known to and used by you;
- ✓ Ensure the active chat window on your desktop is closed at the end of each working day. Users should be aware that all conversations/chats are

purged when the active chat window is closed and/or when logging out of Jabber.

- ✓ Inform your line manager if you feel you have been harassed or bullied, or you are offended by material received from a colleague via Jabber. Information and advice on the Council's Whistleblowing policy and procedure can be found on the Speak up if its not right Staffnet page
- ✓ Take account of the environment you are working in and ensure adequate security regardless of whether you are in the office, at home, in any other location or whilst travelling.
- ✓ Only install/log on to Cisco Jabber on your own device, not on that of a colleague, friend or relative.
- ✓ If using the Cisco Jabber app, ensure automatic updates are enabled.

- ✓ When using the Cisco Jabber mobile app for the first time you **must:**

Apple device

- Click your initials (top left) from the Contacts screen
- Click Settings
- Click Chat List
- **TURN OFF** 'Save Chat List' by toggling the button to the left.

Android device

- Click your initials (top left) from the Contacts screen
- Click Settings
- Click Display
- Select Chat List and **toggle to 'Don't Save'**
  OR this may appear as 'Save Chat List' which you **TURN OFF** by toggling to the left.

8. Things you must not do

- ✘ Make or receive calls in a public place without adequate security precautions, e.g. using headphones, ensuring conversations can't be overheard, etc.
- ✘ Disable, defeat or circumvent any security measure that the council has put in place to protect its information assets, physical assets or reputation.
- ✘ Send messages from another user's account or under an assumed name unless specifically authorised
- ✘ Leave your device unattended and logged on. If not in use, it should be locked, logged out or shut down.
- ✘ Allow your ICT equipment to be used by work colleagues, family members, friends or visitors – staff are personally accountable for anything accessed via their user ID.
- ✘ Use Cisco Jabber to share personal or special category information

- ✘ Allow others to access information and systems they are not entitled to when using the screen-sharing facility.
- ✘ Create content that 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, 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 others.

9. Retention of data

Cisco Jabber/collaborative software is not intended to be a medium for retaining data. All data created for business purposes **MUST** be stored in the relevant council system and held in line with the council's retention schedule.

10. 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.

If a manager or investigating officer believes that collaboration software has been misused, spot checks and/or reports may be produced to support investigations. To obtain activity reports contact the ICT Service Desk.

Any device (council or personal) which provides access to Cisco Jabber, may be confiscated as part of an investigation if there is an allegation of misconduct, in line with the Procedure for Securing and Investigating the content of ICT Equipment.

11. Policy Compliance

Anyone with access to the council's collaborative software 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.

Use of Cisco Jabber 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 activity.

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.

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.

12. Policy Review

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

13. Document Control

Author:	Kirsty Benzie, Assistant Head of IMS (Caldicott Angel)
Owner:	Mandy Quayle, Director of Digital & People Services
Document Number:	V1.1

Revision date	Summary of Changes	Changes marked

December 2020	Add link to Procedure for Securing and Investigating the content of ICT Equipment. Update policy owner details.	V1.1

Document Approvals

Version	Approved By	Date
1.1	Information Board	December 2020