

Purpose

This policy applies to all CCC's employees and workers, contractors, members and agents, and sets out the conditions to use WhatsApp on Council issued or Council managed devices - referred to as *Council Controlled Devices (CCD)*.

The policy is intended to:

- Enable limited use where appropriate
- Protect Council information, systems, and reputation
- Clarify responsibilities and limitations, including Digital Services support boundaries

WhatsApp is not an approved corporate communication tool and must not be used as a substitute for official Council systems.

Scope

This policy applies to:

- All CCC's employees and workers, contractors, members and agents on CCDs
- All Council owned or Council managed mobile phones, tablets, and computers
- Any use of WhatsApp on CCDs, whether for work related or personal purposes

Where authorised by management and supported by a legitimate business need, this policy also applies to employees using WhatsApp for Council-related communications on personally owned devices.

Use of WhatsApp on personal devices shall be limited to low-risk operational communications and must comply with all requirements of this policy.

Policy Statement

The Council permits the installation and use of WhatsApp on CCDs on a tolerated but unmanaged basis.

Key principles:

- Use is at the individual's own risk
- The Council does not manage, approve, or endorse WhatsApp
- All existing Council policies continue to apply, including:
 - Information Governance
 - Data Protection (UK GDPR & Data Protection Act 2018)
 - The Data (Use and Access) Act 2025
 - Code of Conduct
 - Behaviours and Values
 - Acceptable Use

Users must not treat WhatsApp as a corporate records repository and must ensure important business information is transferred to approved Council systems where required.

Support and Service Limitations

Digital Services:

- Will install it
- Does not provide further support for WhatsApp
- Will not assist with:
 - Configuration
 - Account setup, verification, or recovery
 - Q&A, Troubleshooting or fault resolution
 - Message, media, or backup recovery

Any issues with WhatsApp must be resolved by the user directly with the application provider.

Digital Services may remove WhatsApp as part of:

- Security remediation
- Device replacement or reset
- End of employment processes

Digital Services may additionally remove WhatsApp from any Council Controlled Device where security, compliance, operational or information governance concerns are identified.

Acceptable Use

WhatsApp use on CCDs is permitted provided that:

- Managers approve - use is proportionate and incidental
- It does not interfere with work duties
- It does not replace Council approved systems such as email, Teams, service applications, or case management systems
- Council data is not created, stored, or shared inappropriately
- WhatsApp must never be relied upon as the sole record of any work activity or for any emergency communications.

Managers may authorise WhatsApp groups where there is a legitimate operational requirement.

Business-critical information, actions, decisions, instructions and records communicated through WhatsApp must be transferred to approved Council systems without undue delay. Managers should act as group administrators wherever practicable and periodically review group membership to ensure access remains appropriate.

Personal Devices

Employees using WhatsApp for Council-related communications on a personal device must:

- Have a legitimate business need for it.
- Read and comply with this policy.
- Complete the WhatsApp User Acknowledgement process before joining Council WhatsApp groups.
- Ensure appropriate device security measures are maintained, including passcodes, screen locking and any available device encryption.
- Report lost, stolen or compromised devices immediately.
- Cooperate with lawful Council requests relating to Freedom of Information requests, Subject Access Requests, investigations, audits, complaints and legal proceedings.

Prohibited Use

WhatsApp must not be used on CCDs to:

- Share or store:
 - Personal data
 - Confidential or sensitive Council information
 - Information classified as official, sensitive or equivalent
- Transmit:
 - Logins, passwords, PINs, MFA codes, or security details
- Conduct:
 - Formal decision making
 - Approvals or authorisations
 - Instructions affecting service delivery
- Discuss:
 - HR matters
 - Complaints
 - Safeguarding concerns
 - Legal or disciplinary issues
- Engage in behaviour that breaches the Council's Code of Conduct

Personal devices must not be used for routine sharing of confidential, commercially sensitive, safeguarding, special category, criminal offence, HR, disciplinary or legal information.

Special category data must not be routinely processed through WhatsApp.

Information Governance and Data Protection

Users must be aware that:

- WhatsApp data is outside Council control
- Messages and media may be:
 - Automatically backed up
 - Stored offshore
 - Subject to third party access
- End-to-end encryption does not equate to compliance with Council governance obligations

Any actual or suspected:

- Data breach
- Accidental disclosure
- Loss of device containing WhatsApp data

must be reported immediately in accordance with the Council's Information Security Incident procedures.

Users should be aware that mobile telephone numbers may be visible to other group members.

WhatsApp and Meta may process personal data outside the UK, including the United States.

Only low-risk operational information should therefore be communicated through the platform.

Important Council records must be transferred from WhatsApp into approved Council systems in accordance with retention, records management and information governance requirements.

Conduct and Professional Standards

When using WhatsApp on a Council device, users must:

- Always maintain professional behaviour
- Communicate respectfully with colleagues, members, partners, and the public
- Avoid informal or ambiguous messaging that could be misinterpreted or misused
- Remember that private or group chats do not exist outside Council standards

Messages sent via WhatsApp may be disclosable under:

- Freedom of Information legislation
- Subject Access Requests
- Court or regulatory proceedings

Where Council business is conducted through WhatsApp, users may be required to assist in locating and retrieving relevant information.

Use of Council Controlled Devices (CCD)

Council devices:

- Remain the property of the Council
- Are subject to monitoring, audit, and investigation where required
- May be remotely locked, controlled, wiped, or reset without notice for security or operational reasons

Users must not assume WhatsApp data will be preserved.

Privacy Considerations

The Council does not routinely monitor WhatsApp content. However:

- Device activity may be reviewed where justified
- Access may be required as part of investigations or legal requirements
- Use of a Council device does not guarantee personal privacy

Compliance and Breach Management

Failure to comply with this policy may result in:

- Removal of WhatsApp from the device
- Restriction of device usage
- Formal investigation
- Disciplinary action in line with Council procedures

Serious breaches may constitute misconduct or gross misconduct.

Failure to transfer Council records into approved systems, failure to comply with information governance requirements, or inappropriate use of personal devices may be treated as a policy breach.

Review and Governance

This policy will be reviewed:

- Periodically
- Following relevant legislative or technological changes
- Where risks to the Council are identified

Status of WhatsApp for Members

- WhatsApp is not an approved method for conducting Council business, decision making, or casework
- Use of WhatsApp by Members is unmanaged and unsupported by Digital Services

- Use is at the Member's own risk and discretion, subject to statutory and ethical obligations

Members must ensure that WhatsApp conversations do not become the primary record for any Council related matter.

Decision Making and Governance

WhatsApp must not be used by Members to:

- Take or influence formal Council decisions
- Reach collective agreement outside formal meetings or approved processes
- Substitute for properly convened meetings, briefings, or reports
- Circumvent transparency, scrutiny, or constitutional requirements

Members are reminded that decision making must comply with:

- The Council's Constitution
- Local Government legislation
- Principles of openness and accountability

Casework and Resident Communications

Members must not use WhatsApp to:

- Receive or store sensitive resident casework
- Handle safeguarding, licensing, planning, or complaint matters
- Share personal data relating to residents, complainants, or service users

Where residents contact Members via WhatsApp:

- Sensitive matters must be transferred promptly to approved Council systems
- Messages should not be retained solely within WhatsApp
- Members must ensure compliance with UK GDPR and Council information governance rules

Conduct and Standards of Behaviour

Members using WhatsApp must comply with:

- The Members' Code of Conduct
- The Nolan Principles of Public Life
- Council policies

This includes ensuring that WhatsApp is not used to:

- Disclose confidential or exempt information
- Make inappropriate, defamatory, or intimidatory remarks
- Engage in political or party-political activity
- Conduct private discussions that could undermine public trust

WhatsApp messages may be subject to:

- Complaints under the Members' Code of Conduct
- Investigation by the Monitoring Officer
- Disclosure as part of legal or regulatory proceedings

Information Governance and Records

Members are advised that:

- WhatsApp messages relating to Council business may be:
 - Disclosable under Freedom of Information legislation
 - Subject to Subject Access Requests
 - Required for audit, investigation, or court proceedings
- WhatsApp does not meet Council record keeping standards

Members are responsible for:

- Ensuring relevant information is captured in approved Council systems
- Cooperating with any lawful request for information held on Council devices

Breach and Escalation

Failure by a Member to comply with this policy may result in:

- Removal of WhatsApp from a Council device
- Referral to the Monitoring Officer
- Investigation under the Members' Code of Conduct
- Withdrawal of Council IT facilities (where appropriate)

WhatsApp User Acknowledgement – [click here](#).

Document History

Version Number	Creation Date	Changes Made	Changes Made By:	Authorised/Checked	Date of Changes
1	16/04/2026	Doc creation	JR	MS \ JB \ DSB \ LB \ DW (Digital Services, HR, Information Governance Manager, Legal & Democratic	22/06/2026
2	22/06/2026	Content review	JB DW	JR MS	30/06/2026

WhatsApp Use Policy Frequently Asked Questions (FAQs)

This guide provides practical guidance to accompany the [WhatsApp Use Policy](#) and addresses the most common questions raised by employees and managers.

General

1. Why does the Council have a WhatsApp policy?

To ensure WhatsApp is used appropriately, securely and consistently.

2. Has WhatsApp been approved for work use?

WhatsApp is not an approved corporate communication platform but limited use is permitted where there is a legitimate business need.

3. Do I have to use WhatsApp for work?

No.

4. Should Council business move to WhatsApp?

No. Approved systems remain primary.

5. Does the Council manage WhatsApp?

No, it remains a third-party application.

Personal Devices

1. Can I use my personal phone?

Yes, subject to manager approval and user acknowledgement.

2. Can I refuse?

Yes. Discuss alternatives with your manager.

3. Will the Council access my phone?

Not routinely, but work-related information may be required for lawful requests.

Appropriate Use

1. What can WhatsApp be used for?

Low-risk operational messages, attendance updates, logistics and coordination.

2. What must not be shared?

Personal data, safeguarding, complaints, HR, legal, disciplinary and sensitive Council information.

3. Can I discuss customer cases?

No.

4. Can I discuss licensing, planning or enforcement cases?

No.

5. Can I make decisions or approvals on WhatsApp?

No. WhatsApp should not be used for formal decision-making, approvals, authorisations or instructions affecting service delivery. Where a decision needs to be made or approved, this should be done through the appropriate Council process and recorded within the relevant Council system.

Work Groups

1. Can we create work groups?

Yes, where there is a legitimate operational need.

2. Who owns a work group?

The service area.

3. How many admins should there be?

At least two where practicable.

4. Can groups be used for decisions?

No.

5. What happens when staff leave?

Membership should be reviewed and updated promptly.

Private Social Groups

1. Can colleagues have social groups?

Yes.

2. Do social groups require the acknowledgement?

No.

3. What if work is occasionally mentioned?

Incidental references do not normally make it a Council communication channel.

Privacy and Data Protection

1. Can others see my number?

Yes.

2. What if I do not want my number shared?

Discuss alternatives with your manager.

3. Is WhatsApp automatically GDPR compliant?

No.

4. Does encryption remove risks?

No.

Security

1. What security should I use?

PIN/password, biometrics, device locking and updates.

2. Lost device?

Personal phone - report to your manager immediately

CCC work phone - [report to Digital Services immediately](#)

3. Sent information to the wrong person?

Report as a [security incident](#) immediately.

Records Management

1. Can WhatsApp be the official record?

No.

2. What if important information is discussed?

Transfer it to a Council system.

3. Can messages be requested under FOI or SAR?

Potentially yes.

Working Hours and Support

1. Must I monitor WhatsApp out of hours?

No, unless agreed as part of your role.

2. Can I mute groups?

Yes if operational duties are unaffected.

3. Does Digital Services support WhatsApp?

Digital Services provides limited support for WhatsApp installation and access on approved CCC mobile phones only. WhatsApp group management remains the responsibility of the relevant service and its administrators.

4. What if I stop using WhatsApp?

Speak to your manager.

Myths and Facts

1. Myth: WhatsApp is now the Council official communication system.

Fact: Approved Council systems remain the primary communication methods.

2. Myth: Messages on my phone cannot be requested.

Fact: Work-related information may still be disclosable.

3. Myth: Work groups belong to whoever created them.

Fact: They belong to the service.

4. Myth: I must sign the acknowledgement for a friends group.

Fact: Genuinely private social groups fall outside the arrangements.

5. Myth: Encryption means compliance.

Fact: Governance obligations still apply.

Practical Examples

Acceptable examples: running late, working from home, meeting venue changes, arranging site attendance, rota or shift updates, operational coordination.

Not acceptable examples: resident information, safeguarding concerns, complaints, HR issues, legal advice, disciplinary matters, passwords, formal decisions and approvals.

Who can help?

For advice contact your Line Manager, [Digital Services](#), [Information Governance Team](#) or [HR](#) as appropriate.