Appendix 3

WhatsApp Policy Draft v0.2

Contents

WhatsApp draft v0.2

Introduction and aims

This guidance aims to:

1. Facilitate efficient and modern day-to-day communication
2. Manage risks to the security of information
3. Aid compliance with the principles of record-keeping, accountability and transparency

Adopting evolving modern technology means we can support our operation to stay effective over time. As a result, the councils have approved WhatsApp for use under the specific circumstances as set out in this document.

This guidance sets out when it is and is not acceptable to use WhatsApp, and how to reduce the risks of using it. Staff must follow this guidance.

WhatsApp is the market leading messaging app people use to share information. Any channel that allows us to communicate effectively offers significant opportunities. The risks to mitigate are also significant, as inappropriate or in non-compliant use could lead to:

- **Legal risks** of penalties to staff and the councils
- **Reputational risks** for the councils
- **Data breaches**.

For these reasons, WhatsApp is only permitted for the narrow band of uses as set out in this document, where it helps to meet a particular need to communicate. In general, WhatsApp should be considered a last resort for work purposes, to be used when there is no viable alternative across the systems the councils provide for work purposes.

Please remember that WhatsApp is a social media application, and is therefore also covered by our Social Media Policy.

Any deviation from this guidance must be backed up by a risk assessment with a strong justification or rationale.

Summary

You can use WhatsApp at work for non sensitive information only and with care. See below for a guide to what is non sensitive information.

When talking to	About	Use WhatsApp
Internal colleagues	Sensitive information	Never
	Non-sensitive information	With care
Official partners	Sensitive information	Never
	Non-sensitive information	With care
Customers	Sensitive information	Never
	Non-sensitive information	Never
The public	Sensitive information	Never
	Non-sensitive information	Via corporate Communications

‘With care’ means with due care, attention, and forethought to the contents of your conversation, particularly the risk of committing a data breach by including sensitive information including through unexpected data in the background of shared photos.

When information is ‘sensitive’

As council employees, our data at work is automatically classified under government security rules as OFFICIAL. This means you can never just share work data, and rules will always apply to it. However under OFFICIAL there are two levels of ‘sensitivity’: OFFICIAL SENSITIVE and OFFICIAL NON SENSITIVE.

Here are examples:

OFFICIAL SENSITIVE	OFFICIAL NON SENSITIVE
Anything with recordkeeping requirements including under the GDPR and FOI, i.e. most data and normal business of the council.	Logistical communications, office admin, service info (e.g times, locations), info for public release (e.g news, photos, PR), promotional

E.g. customer service interactions, personal data, aggregated data, internal council data, decisions, transactions.	info (e.g. adverts, offers), dataless information.

These lists are not exhaustive.

In general, you must treat all council information as sensitive unless and until you exercise your professional judgement that it is non sensitive. You should expect to be able to defend your judgement on this if challenged. If in doubt, always treat information as sensitive.

Ask yourself

1. Do I really have to use WhatsApp for this? Is there any way I can avoid it?
2. Is there already a corporate system I could use for this, like Email or Teams?
3. Is this data definitely non-sensitive?
4. Would I be happy for this to be made public?

Examples

Example A: team group chat

WhatsApp can be helpful to share information within a team, for example, to alert to a change in venue for a meeting, arrange cover if someone is running late / off work / at late notice, or alert a team to information shared on another channel that they need to be aware of. All this kind of information would be non sensitive, and therefore permitted with care.

Such a chat must not however be used for any personal or confidential information relating to staff, customers, or the business of the council – all of which would be sensitive information, and never permitted. That business would have to be conducted via council systems.

Example B: "I've sent you an email that needs action"

WhatsApp can be helpful to alert someone, for example a partner, councillor, or someone you know is out in the field, to urgent information you have sent via another channel.

For example, you might need to say "I've sent you an important work email that needs attention by midday". That is non sensitive information. The sensitive contents of that email, however, would never be OK to share on WhatsApp.

Remember

- You are subject to work policies at work, including the Code of Conduct and Social Media Policy.
- If you become aware of misconduct at work, it is your responsibility to report it.
- Remember to remove leavers from your team chats, as they have become external customers!
- Stay cyber savvy and be vigilant to the ever-present threat of scams and phishing.
- WhatsApp is not secure: once sent, content is out in the public domain and cannot be removed and there are no deletion guarantees anywhere.

- Even with ‘disappearing messages’ turned on – i.e. when messages are removed from the sender and receiver’s phones after a certain period – you have no way to know what has happened to the data once you press send.
- WhatsApp’s operator, Meta, stores data on the sender and receiver: their location, phone numbers, contact lists. Meta cannot see or access the content of messages.

If you accidentally share sensitive data on WhatsApp

If you think you have accidentally shared sensitive information on WhatsApp, it could be a data breach.

1. Don’t panic
2. Delete the suspect message(s)
3. Delete any related media from your phone
4. Delete any cloud backups of that media your phone may have performed
5. Inform your line manager that you have done the above and what happened, so our processes around a potential data breach can be followed.

Photos via WhatsApp

In general, you should not include anything of a confidential or sensitive nature in shared images on WhatsApp.

Images of people are sensitive by default. They contain personal data with significant implications, including under the GDPR. There is a simple process to achieve compliance for sharing images. That includes completing an online photo consent form at www.bromsgrove.gov.uk/photo or www.redditchbc.gov.uk/photo. Contact Communications for further advice on this.

Using your own device? Know the risk

If you are using your own phone for WhatsApp, for example if you don’t have a compatible work phone, understand that any device you use for sensitive council data could become subject to Freedom of Information (FOI) requests.

Calls and video calls via WhatsApp

In general, avoid using these. But in an emergency when there is no mobile signal but there is Wi-Fi, you can use this feature. Be aware of the usual risks of data breaches around audio and video calls (e.g. having sensitive data overheard by people who should not have access to it, or having sensitive data shared on screen or visible in the background),

Emergency Response: WhatsApp usage

The following has been provided by Applied Resilience and applies specifically to the use of an Emergency Response WhatsApp group.

Purpose

If action is required in a civil emergency. a message will be posted in the Emergency Response WhatsApp group. This allows the initial rapid notification of users in the group. Following the notification, the relevant group members will then be contacted by Applied Resilience via phone to ensure notification has been received. Ongoing general updates may be posted on the group in line with the guidance below.

Information that can be shared

The sharing of non-identifying, non-sensitive information can be shared within the group relating to the emergency. The primary purpose of the group is for initial notification and general updates.

Information that cannot be shared

Any identifying or sensitive information cannot be shared in this group. This includes personal details of affected residents. Adherence to GDPR policy must take place. If sensitive data needs to be shared, this should be done either via the phone or through email.

Data retention

Data in the group is retained for # years after which point it is deleted. The responsibility will be on the message sender to delete messages after the # year time limit is reached. If there are any changes to this timeframe you will be informed by one of the group administrators. If an incident is going to enquiry, then messages will be retained for the duration of the enquiry.

Group administration

The group administration will be undertaken by NAMED OFFICERS and Applied Resilience. If you no longer require access to the group for reasons such as, leaving the council, change in job role, or no longer forming a part of the response, please contact one of the above to be removed unless you have already been removed. Contact details will be updated upon the review of the Emergency Contacts Directory, however, if you have a change in details, please contact one of the administrators.

If you have any questions or queries, please contact the group administrators listed above.

Sources

1. West Mercia Police - internal WhatsApp policy
2. Cabinet Office Cabinet Office guidance for the use of Non Corporate Communications Channels (March 2023)
3. Cabinet Office Guidance 1.1: Working at OFFICIAL (Aug 2024)
4. West Mercia LRF - Rebecca Pritchett
5. Applied Resilience - Nick Moon and Robin Churchill