WhatsApp in the Workplace – what you should know

Overview

WhatsApp has increasingly become the 'go-to' platform for communicating with friends and family – organising nights out (or in) and sharing photos. It's also come in useful for keeping in touch with colleagues during this extended period of home-working as well as being used to pass information to our volunteers and other staff in the field. This form of real-time informal workplace communication can benefit the Authority in several ways. Primarily, it can improve the social connection we have with each other and our place of work, encouraging collaboration and providing an opportunity for mutual support. It is especially beneficial for teams with remote workers and those who work differing hours and shifts.

However, there's a darker side to WhatsApp – a growing number of legal cases involving bullying or harassment have stemmed from conversations that have taken place on the platform. It can be a great benefit for employees as long as it's used for the right reason. It can, however, be too easy for people to act inappropriately and find themselves in breach of policies without realising the impact of their behaviour. Ensuring that you are sharing information appropriately and with the right people is key – data protection rules and obligations of confidentiality don't just disappear when using WhatsApp and bear in mind that chats may be caught by Freedom of Information legislation. Apply the same etiquette to WhatsApp messages as you would apply to any other work correspondence:

- Think before you include personal or confidential info/images in a chat – you might have deleted the chat, but the recipients could still have it
- Remain professional; use neutral, professional language and tone
- Avoid ill-advised comments on individuals and ensure that you differentiate between fact and opinion
- Refrain from angry chats
- Take care to ensure that the content of the chat cannot be interpreted as harassment, discrimination or abuse
- Refer to the Information Management Policies Framework which provides acceptable use guidelines for social media

WhatsApp Security features:

The following are some of WhatsApp's security features (including links to tips on strengthening the security):

WhatsApp and consent – saying 'OK' to allowing access to your phone contacts when setting up the app will upload the numbers of all your contacts to the WhatsApp servers (in the US or Ireland). Communicating with work colleagues using WhatsApp assumes that they are comfortable with downloading and corresponding via the app. There is some 'implied' consent in this, but everyone needs to be aware of the information uploaded to the WhatsApp servers (contact details), the information that is stored on your phone and the information that is shared (all chat content).

Data Portability – you can request your own account information, but this does not include your message history.

Account Deletion – you can delete your account information and profile photo. Deleting your account will remove you from all groups, delete undelivered messages and delete the message history held on the phone and in an iCloud or Google drive backup (if set).

End-to-end Encryption – applies to messages in transit and is set to on by default. Encryption ensures that only the sender and the recipient can read the message. Third parties can't and neither can WhatsApp. WhatsApp has no password locks for accounts, so be careful whom you allow to use your phone – apply a PIN code and if you can, enable Touch ID or Face ID lock (on iPhone) or Fingerprint Lock (on Android). You can add an extra layer of security by setting up two-step verification. If however, someone gets hold of your phone and you have not put any security around it, or WhatsApp, then the chats you've sent and those you've received can be read. **If you lose your work phone, it can be remotely wiped so please ensure you report the loss to IT Support.**

Deletion of messages - delivered messages are automatically deleted from WhatsApp's servers, including chats, photos, videos, voice messages, files and location information shared with your contacts. Messages however, will be retained in a backup (iCloud or Google drive) if you have set this. Chats are retained on the WhatsApp servers until they can be delivered; if a message is on the WhatsApp servers for more than 30 days it is deleted.

Inactive accounts – any account which is inactive for 120 days is deleted

Restriction on forwarding chats – when you forward a message you can share it with up to five chats at one time. However, when a message is forwarded through a chain of 5 or more chats (meaning it's at least 5 forwards away from its original sender) the message is labelled with a double arrow icon. These messages can only be forwarded one chat at a time, as a way to help keep conversations on WhatsApp more private and personal

Sending photos – whilst there isn't any functionality in WhatsApp to stop users sending photos, it is possible to make sure that photos aren't automatically saved to your phone's photo gallery. To change the settings so that images are not saved, follow the guidance here. Changing the settings will also help to reduce the amount of storage that is used by WhatsApp.

Further details on controlling your privacy including managing your profile photo, group privacy settings and status updates, can be found here.