Scottish Government
Riaghaltas na h-Alba
gov.scot

Mobile Messaging Apps

Usage & Policy

Version 2.1
Last Update November 2021
Author Information & Technology Services Division

Contents

1. What are Mobile Messaging Apps?

1.1 Mobile messaging apps are software applications installed on a telephone or mobile device that enable text (and often other forms of) communication between users using the same application. This includes the text facility on mobile phones and apps such as WhatsApp, Viber, Telegram and Signal. Many other products are available and the marketplace changes rapidly

1.2 Social media platforms such as Facebook also use mobile messaging within them, but these are not always secure platforms on which to have conversations regarding government business. For this reason, **we strongly advise against using any chat tools within social media platforms**.

2. Usage of Mobile Messaging Apps in a business context

2.1 Mobile messaging apps can be a useful tool for supporting the delivery of business, particularly in an acute context, e.g. business continuity or staff welfare.

2.2 Scottish Government does not therefore prohibit usage of mobile messaging apps but requires a proportionate approach from staff, contractors and Ministers that balances the benefits and risks of mobile messaging depending on the purpose for which they wish to use it (e.g. using it in an emergency versus as a general regular communication tool). **Everyone using these apps must be aware of important considerations around the usage of the apps**, including:

- The transfer of sensitive data across unregulated servers outside the European Economic Area (EEA);
- Compliance with data protection requirements regarding 'fair processing and individuals' rights, ;
- Compliance with records management responsibilities and legislation – including the Public Records (Scotland) Act 2011;
- Compliance with obligations under the Freedom of Information (Scotland) Act 2002;
- Data security risks when using non-SCOTS devices.

3. Choice of App – Security & Privacy

3.1 The security features of a mobile messaging app can help ensure that your message stays private between you and the intended recipient or recipients. The following features are particularly important if your message contains information that could potentially be used to identify an individual or would cause reputational harm to government.

- **Encryption** – does the app meet the NHS end-to-end encryption standard of "AES 256"?
- **End-user verification** – can the app verify that the people using the app are indeed who they say they are?
- **Passcode protection** – can a secondary PIN be used to protect the app, and can it be time-out enabled?
- **Remote-wipe** – can the messages be removed if the device is lost, stolen or redeployed to another staff member?
- **Message retention** – does the app allow automatic deletion of messages after a set period of time?

3.2 Due to the lack of most of these features in the standard texting applications for mobile phones, **we strongly advise against the use of SMS text messages for business purposes - other than notification for staff about business continuity or issues with buildings or infrastructure – e.g. urgent closure of a building or issues with IT systems.**

3.3 A comparison of the security features of the current most-used apps is given in the table below. Please note that we have not tested the features of all of these apps - we are simply reflecting what was stated on their websites at the time of publication.

	End-to-End encryption (AES 256)?	Passcode protection?	Remote wipe?	Message retention – automatic deletion?
WhatsApp	Yes	Not on app	No, but account can be deactivated	Secret conversation
Viber	Yes	Yes, on hidden chats	No	Yes
Telegram	Yes (letter-sealing feature)	Yes	Yes	Yes
Signal	Yes	Yes, on Android	Not Known	Yes

4. Records and Information Governance

4.1 Mobile messaging does not change your responsibility within Scottish Government to maintain complete and comprehensive records of key conversations and decisions. Therefore, at least monthly but preferably at the earliest opportunity**, you must transcribe the salient points of any business discussions and/or decisions in a mobile messaging app into an email or text document using the SCOTS platform and save this to the Electronic Records and Document Management system (eRDM).** Failure to keep and track official records under an agreed retention and disposal schedule is not good business practice and risks non-compliance with the Public Records (Scotland) Act.

4.2 **You must also consider whether aspects of a mobile messaging app conversation should be transcribed to SCOTS for Freedom of Information requests.**

4.3 **At least monthly, after having followed the guidance in the above paragraphs, you must delete business conversations in the mobile messaging app** – i.e. no business conversations should be retained in the app for more than one month.

5. Responsibilities for Group Chats

5.1 It may often be the case that business areas or members of particular teams will be participants in a group chat on a mobile messaging app. In this event, **the group should nominate a Group Responsible Owner (GRO) for the chat group**.

5.2 **At least once a month the Group Responsible Owner should publish a message to the group to remind all participants of their obligations**. This would usually say something along the lines of:

> "Colleagues, this is your regular reminder that conversations in your government capacity on any platform are subject to FOI, DPA and public records legislation. Please now review messages from the past month in this group and determine whether any discussions or decisions should be transposed into an official record on the SCOTS platform. After ensuring this has been done, you should delete the conversation from this app.".

5.3 **Where no Group Responsible Owner has been agreed, the most senior chat group participant will be deemed Group Responsible Owner.**

6. The Role of the Information Asset Owner (IAO)

6.1 Across Scottish Government, information governance is overseen largely at Information Asset Owner level – which will normally be at Deputy Director or Director level. Information Asset Owners have responsibility for the information assets held by their Division or Directorate at a local level and are required to report on information governance during completion of their annual Certificates of Assurance exercise.

6.2 **You should make your Information Asset Owner aware that you are using a mobile messaging app for business purposes** and seek guidance from them on best practice - based on the purpose of business conversations and/or groups.

6.3 **Should there be any incidents where data, messages or conversations are inadvertently shared incorrectly or cause any problem – then you must inform your Information Asset Owner** that an incident has occurred. This will enable them to make an impact assessment of the situation and potential repercussions.

7. General Good Practice for Mobile Messaging Apps

7.1 Minimise the amount of personal or confidential information you communicate via mobile messaging.

7.2 Set your device to require a passcode immediately, and for it to lock out after a short period of not being used.

7.3 Do not allow anyone else to use your mobile device is you use a mobile messaging app for business purposes.

7.4 Wherever possible use additional security settings for mobile messaging apps – such as additional PIN codes or two-step verification.

7.5 Disable message notifications from the mobile messaging app from appearing on your device's lock-screen.

7.6 Enable the remote-wipe feature in case your device is lost or stolen. You should be aware however that using this feature means that everything is deleted from your phone, including contacts and photos.

7.7 Always ensure that you are communicating with the correct person or group - especially if you have similar contacts stored in your personal device's address book.

7.8 If you are a mobile messaging app group administrator, take great care when selecting the membership of the group and review membership regularly.

7.9 Separate your personal and social groups on mobile messaging apps from any groups that share business or operational information.

6.10 Review any links to other apps that may be included with the mobile messaging software and consider whether they are best switched off.

6.11 Remember that if you use your personal device for business communications, losing it will potentially have business as well as personal ramifications.

8. Summary of Advice and Required Actions when using Mobile Messaging Apps

Ref.	Action / Advice
1.2	We **strongly advise** against using any chat tools within social media platforms.
2.2	Everyone using mobile messaging apps **must** make themselves aware of the important legislative and security considerations around the usage of the apps.
3.1	You **must** consider and assess the settings within the mobile messaging app to help safeguard the integrity of any business information. These include enabling encryption, end-user verification, passcode protection, remote-wipe, and automatic message deletion.
3.2	We **strongly advise** against the use of SMS text messages for business purposes other than notification for staff about business continuity or issues with buildings or infrastructure.
4.1	You **must** transcribe the salient points of any business discussions and/or decisions in a mobile messaging app into an email or text document using the SCOTS platform and save this to the Electronic Records and Document Management system (eRDM).
4.2	You **must** consider whether aspects of a mobile messaging app conversation should be transcribed to SCOTS for Freedom of Information interests.
4.3	You **must** delete business conversations at least monthly in the mobile messaging app.

5.1	For Group Chats the group should nominate a Group Responsible Owner (GRO) for the chat group.
5.2	At least once a month the Group Responsible Owner should publish a message to the group to remind all participants of their obligations in terms of information governance.
5.3	Where no Group Responsible Owner has been agreed for a Chat Group the most senior chat group participant will be deemed to be GRO.
6.3	Should there be any incidents where data, messages or conversations are inadvertently shared incorrectly or cause any problem – you **must** inform your Information Asset Owner.

9. Further Help and Guidance

9.1 For further information please see additional links below or log an iFix request for iTECS advice at iFix Portal - Home

9.2 **Data handling and SG IT Code of Conduct**

All Scottish Government data should be handled in accordance with the -

Scottish Government data handling standard

and the -

Scottish Government IT Code of Conduct

9.3 **Transmission of personal data**

If any personal data is likely to be transmitted via a proposed chat group on a Mobile Messaging App, Cyber Security & Information Assurance colleagues recommend that a GDPR data protection impact assessment is conducted and signed off by the relevant Information Asset Owner to identify any privacy risks before using the App.