HM Government

Using non-corporate communication channels (e.g. WhatsApp, private email, SMS) for government business

Introduction

1. This guidance supersedes *Guidance to departments on the use of private email*. It communicates government policy and promotes good practice with the following goals:
    a. To facilitate efficient day-to-day government discussions in a modern way;
    b. To reduce risks to the security of information;
    c. To comply with the principles of good government, including record-keeping, accountability and transparency.
2. Departments must link to this government-wide guidance in their guidance to staff and may provide additional advice if required by their specific risk environment.
3. This guidance applies to central government and arm's length bodies. It applies to all individuals in central government (ministers, special advisers, officials, contractors, non-executive board members and independent experts advising ministers).

Policy principles

4. Departments should, as far as reasonably practicable, enable approaches in their core systems that reduce the need for NCCCs.
5. Government communications belong to the Crown and must be handled lawfully. If you hold such communications in NCCCs you do so on behalf of your department.
6. This guidance requires you to exercise professional judgement appropriate to your circumstances, including with regard to the codes of conduct and legal obligations which apply to you and the post you hold within your department. Use NCCCs with care and be prepared to explain and defend your choices.
7. All government information has a classification (even if not formally marked) and falls within the Government Security Classifications Policy. You must observe any restrictions applied to information, such as Handling Instructions or Descriptors.

Appropriate use of NCCCs

8. In general, it is expected that you use government systems for government business. Any use of NCCCs for significant government business engages your recordkeeping responsibilities.
9. If you are accessing a NCCC on a corporately managed device:
    a. **Particular care** should be applied if communicating significant government information; and/or information with additional marking (including information marked -SENSITIVE) requiring additional protective controls or behaviours.

b. You should use your **discretion, exercising professional judgement** if communicating any logistical or other non-significant government information.

10. If you are accessing a NCCC on a privately owned and managed device:

    a. You would require **exceptional circumstances** to justify communicating significant government information; and/or information with additional marking (including information marked -SENSITIVE) requiring additional protective controls or behaviours. Any use in these circumstances should be reported to your Knowledge and Information Management team and Head of Unit.

    b. You should **pay due regard to your security responsibilities** if communicating any logistical or other non-significant information.

11. Information classified "SECRET" or "TOP SECRET" must not be shared via NCCCs.

Appropriate use of NCCCs - Summary table

<table>
<tr><td colspan="2">Columns describe the information carriers.

Rows describe the information.</td><td>Accessed via a corporately managed device</td><td>Accessed via a privately owned and managed device</td></tr>
<tr><td colspan="2">SECRET or TOP SECRET</td><td colspan="2">Must not use</td></tr>
<tr><td rowspan="2">OFFICIAL</td><td>Significant information

and/or

Information with additional marking requiring protective controls or behaviours (including information marked -SENSITIVE)</td><td>Particular care required with due regard for recordkeeping responsibilities</td><td>Only in exceptional circumstances.

Any such use should be reported to your Knowledge and Information Management team and Head of Unit</td></tr>
<tr><td>Logistical or other non-significant information</td><td>Permitted</td><td>Permitted with due regard to your security responsibilities</td></tr>
<tr><td colspan="4">Any use of NCCCs must always involve your discretion, exercising professional judgement.</td></tr>
</table>

Definitions and scope

12. 'Government systems' are corporately-overseen systems providing corporate access to the information held in them. In contrast, an NCCC is a communication channel that does not provide corporate access to information.

13. Examples of NCCCs include WhatsApp, Signal; private email; private messaging on social media platforms e.g. Facebook or LinkedIn; and SMS text messaging. This guidance applies to all current and future NCCCs.

14. 'Significant government information' is information that materially impacts the direction of a piece of work or that gives evidence of a material change to a situation.

15. 'Devices' includes desktop PCs, laptops, tablets and mobile phones. This guidance covers the use of NCCCs from any device regardless of ownership and management.

16. Corporate devices are corporately owned and managed: they are generally configured, controlled and updated by government IT service staff.

17. Privately owned devices are owned by individuals and can be either:
    a. Privately owned but corporately managed: where an individual allows the organisation a degree of control / monitoring to improve security.
    b. Privately owned and managed with no corporate management.
18. This guidance does not cover the use of NCCCs for personal, political, constituency or parliamentary purposes. Where such conversations on NCCCs 'drift' into government business, individuals must consider the responsibilities outlined below.

Recordkeeping considerations

Your recordkeeping responsibilities

19. Significant government information in NCCCs should be captured into government systems to support accountability. You are responsible for deciding whether this applies to each communication using professional judgement and considering the context.
20. You may receive unsolicited communications via NCCCs. If a conversation becomes more significant, consider switching to a government system or making sure significant content is subsequently captured within a government system.
21. How to capture significant information:
    a. Copy, forward, screenshot or export it to a government system, OR
    b. Record its substance in a message, note or document on a government system
22. If you are a minister or a senior official, consider including private office staff in communications groups and tasking them to undertake such capture.
23. Capture significant information into government systems at a frequency appropriate to the content and context, including how often you use the NCCC. You should carry out a final review before you change device or leave your post.
24. 'Disappearing message' functions have a role in limiting the build up of messages on devices. You must ensure that any such use does not impact on your recordkeeping or transparency responsibilities.

Departmental recordkeeping responsibilities

25. Departments should ensure that government information is managed lawfully, acting in line with the *Code of Practice on the Management of Records* and having regard for the Records Collection Policy of The National Archives.
26. In particular departments should:
    a. ensure that individuals understand how to capture significant government communications sent via NCCCs;
    b. advise their ministers and senior officials to work with their private office staff to make sure their office routines support recordkeeping responsibilities.
27. Departments should ensure that offboarding procedures remind individuals of their obligations regarding any government information that individuals may have in NCCCs when they leave their department. Ministers leaving office should be reminded of the provisions of the Ministerial Code regarding the return of departmental papers.

Transparency considerations

Your transparency responsibilities

28. Government information held on NCCCs could become the subject of an information access request. Where relevant, departments may ask you to search NCCCs. Deletion or concealment of material relevant to an information request may be a criminal offence.

29. Your department is responsible for deciding what constitutes a reasonable search and will, consulting you as appropriate, decide on exemptions which may apply to any information in scope.

Departmental transparency responsibilities

30. When responding to information access requests, departments should consider if relevant information may be held in NCCCs. Departments should record the nature and extent of the searches conducted when responding to such requests.

Security considerations

Your security responsibilities

31. You should read this guidance alongside security and data protection guidance.

32. Government communications, even at OFFICIAL level, are a potential target for attack. Corporately managed devices are generally more secure than privately owned and managed devices. You must take account of the ‘Appropriate use of NCCCs’ section before deciding on the device you use to access an NCCC.

33. Some NCCCs are more secure than others. Messaging services that deploy end-to-end encryption are likely to be more secure than social media messaging and consumer email services. Private email accounts are frequently targeted by hostile actors. You should consider these factors when deciding whether it is appropriate to use any particular NCCC.

Departmental security responsibilities

34. Departments should implement mitigation for individuals whose communications are particularly attractive to hostile actors.

Data protection considerations

Your data protection responsibilities

35. You must respect the data protection principles: that personal data is kept securely (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage); is only processed lawfully, fairly and transparently; is processed only for the purpose for which it was collected; is kept no longer than is needed; is accurate; and is the minimal personal data necessary for the purpose.

36. You must follow departmental data protection advice when holding personal data on NCCCs. Give particular attention to whether the data is transferred outside of the UK.

Departmental data protection responsibilities

37. Departments should monitor and mitigate data protection risks caused by NCCCs and report notifiable breaches to the ICO. Departments should ensure that NCCCs are not routinely used to process personal information.

Review

38. This guidance will be reviewed on or before 31 December 2025.

CABINET OFFICE

30 March 2023