DWP SMS Text Policy

Chief Security Officer

Department for Work & Pensions

ThinkSecure

The DWP SMS Text Policy is part of a suite of policies designed to promote consistency across the Department for Work and Pensions (DWP) and supplier base with regards to the implementation and management of security controls. For the purposes of this policy, the term DWP and Department are used interchangeably.

Security policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-standards.

Security policies cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

Table of Contents

Policy Title

DWP SMS Text Policy

Overview

The DWP SMS Text Policy informs users on the information which can be sent via SMS (Short Messaging Service) text messages. The policy aims to:

- Inform what data can be sent via SMS Text messaging
- Inform who can send SMS text messages
- Inform when SMS text messages can be sent
- Ensure DWP Acceptable Use and Information Management Policies are followed

Purpose

This policy informs the sending of SMS text messages from DWP Devices and the Text Messaging Application (TMA) on behalf of and when representing DWP. The policy aims to ensure that SMS text messages are sent by the correct means, to the correct correspondences and notes the data which can be sent through SMS text messages. The policy also labels the use of DWP mobile devices through the DWP Acceptable Use Policy and the DWP Information Security Policy.

Scope

The policy applies to all members of DWP staff and its representatives, including contractors, suppliers, or anyone required to send SMS text messages from DWP mobile phones or through the Text Messaging Application (TMA) for DWP business.

This policy does not replace any legal or regulatory requirements.

Policy Statements

1. Users must not use personal mobile phones to contact citizens or customers by SMS text message. Paragraph 8.5 of the DWP Acceptable Use Policy refers.
2. Users must not use DWP Mobile Devices to contact citizens or customers by SMS text message.
3. The use of SMS texting via the Text Messaging Application (TMA) is appropriate when it is being used to give citizens routine, non-personal, business information and reminders.
4. SMS text messaging must not be used for the exchange of personal information with citizens (outbound and inbound). Users must consult the DWP SMS Text Policy Checklists | DWP Intranet to ensure excess data is not sent via SMS text messages. Users must not request personal information from customers via SMS Text Messaging.
5. SMS text messages from DWP mobile devices can be used to conduct business with third parties where there is a business requirement to do so.
6. SMS Text Message templates must be reviewed and authorised by the Customer Communications Team prior to use.
7. When sending text messages via the Text Messaging Application (TMA) the guidance issued by the appropriate business area must be followed. Free text fields must only be used for the purpose they were created for, which have been agreed by the business area and the Customer Communications Team.
8. The Department permits the limited use of web links (URLs) in SMS text messages to citizens. However, the following must be adhered to when including links in SMS text messages to citizens:

    8.1. Web links must only be used when they are completely necessary to deliver the business requirement and must be checked for accuracy by the Customer Communications Team.

    8.2. Users must only send web links which point to the GOV.UK domain or to domains hosted by suppliers and their third parties in relation to work being carried out on behalf of DWP.

    8.3. Users must send the full website address (web link) as opposed to a shortened version.

8.4. Users must not use the “free text” fields in the Text Messaging Application (TMA) to send web links to citizens.

8.5. Users must not include QR codes.

9. The protocol for record management of SMS text message communications must be clearly established and followed in compliance with the Information Management Policy.

10. Use of DWP mobile phones for SMS texting must apply the following protocols to maintain a professional standard and not risk compromising the personal safety of staff or citizen information:

10.1. Users must refer to the government guidance on planning and writing text messages and emails.

10.2. SMS texts must not be sent to landline numbers and must only be sent to mobile phone numbers.

10.3. Citizen contact details must be periodically reviewed in line with DWP retention periods and deleted manually, (if not automatically) once there is no longer a business reason to retain them.

Accountabilities and Responsibilities

a) The DWP Chief Security Officer is the accountable owner of the DWP SMS Text Policy and is responsible for its maintenance and review, through the DWP Deputy Director for Security Policy and Data Protection.

b) It is the line manager’s responsibility to take appropriate action where non-compliance to policy is identified as detailed in the DWP Discipline Policy.

c) DWP staff, contractors and anyone required to use the DWP SMS texting service users are responsible for understanding the requirements contained within this policy and the consequence of non-compliance as defined within.

Compliance

a) All DWP employees, whether permanent or temporary (including DWP's contractors) have security responsibilities and must be aware of, and comply with, DWP's security policies and standards.

b) Many of DWP's employees and contractors handle sensitive information daily and so need to be enacting minimum baseline behaviours appropriate to the sensitivity of the information. Most security incidents and breaches relate to information security.

c) Failure to report a security incident, potential or otherwise, could result in disciplinary action and, in the most severe circumstances, result in dismissal. A security incident is the attempted or actual unauthorised access, use, disclosure, modification, loss or destruction of a DWP asset (or a supplier asset that provides a service to the Authority) in violation of security policy. The circumstances may include actions that were actual, suspected, accidental, deliberate, or attempted.

d) DWP's Security and Data Protection Team will regularly assess for compliance with this policy and may need to inspect physical locations, technology systems, design and processes and speak to people to facilitate this. All DWP employees, agents, contractors, consultants, business partners and service providers will be required to facilitate, support, and when necessary, participate in any such inspection. DWP Collaboration and Communication Services will use software filters to block access to some online websites and services, additional information can be found here DWP Employee Privacy Notice.

e) An exception to policy may be requested in instances where a business case can be made to undertake an activity that is non-compliant with DWP's Security Policies. This helps to reduce the risk of non-compliant activity and security incidents. If an individual is aware of an activity that falls into this category, they should notify the Security Policy and Standards Team immediately.

f) SMS text messages issued on behalf of DWP may be monitored. All other relevant security policies should be read where appropriate, but not limited to those detailed below, in conjunction with this policy:

Information Management Policy

Acceptable Use Policy

Civil Service Code (link is external)

Standards of Behaviour