CWS-CARES System: Acceptable Use Policy

Effective Date: 07/31/2025

Purpose

This Acceptable Use Policy (AUP) outlines the responsibilities and expectations for individuals authorized to access the Child Welfare Services – California Automated Response and Engagement System (CWS-CARES). Its purpose is to ensure data security, privacy, compliance with applicable state and federal laws, regulations, and agency policies.

Scope

This AUP applies to all individuals granted access to CWS-CARES.

System Access and Security

1. Follow all authentication and security protocols required by CWS-CARES system; bypassing security measures is strictly prohibited.
2. Access the CWS-CARES system using assigned credentials and protect login information.
3. Update passwords regularly to maintain system security.
4. Use the CWS-CARES system only for official child welfare business - personal, political, or commercial use is not permitted.
5. Lock devices that access CWS-CARES when stepping away from them to prevent unauthorized access.
6. Do not Introduce any form of malware, viruses, or any content that disrupts CWS-CARES operations. Such conduct violates California Penal Code Section 502 and may lead to disciplinary action, civil liability, or criminal prosecution.
7. Never alter or manipulate system functionality without explicit authorization.
8. Report any system vulnerabilities or identified security flaws immediately.
9. Refrain from uploading executable files (e.g., .exe/program files) or potentially harmful content to the CWS-CARES system.

Responsible Use of Data

1. Treat child welfare data as sensitive – limit access to CWS-CARES data to those with a need-to-know.
2. Do not disclose CWS-CARES data to unauthorized individuals or post it on social media without prior approval from the CWS-CARES Data Owner.
3. Refrain from transferring CWS-CARES data to unauthorized devices, storage locations, or platforms (e.g., personal cloud storage, public sites).
4. Share or export CWS-CARES data only with proper authorization for approved purposes.
5. Do not access CWS-CARES system outside the United States.
6. Do not use the CWS-CARES system for personal gain or activities unrelated to child welfare services that involve unlawful, defamatory, fraudulent, invasive or infringing purposes.
7. Do not share confidential child welfare information with unauthorized individuals.

Best Practices and Guidelines

1. Use secure networks or VPNs when accessing CWS-CARES system; avoid public Wi-Fi.
2. Promptly report suspected misuse or policy violations to your Information Security Officer or raise a CARES support ticket, as needed.
3. Ensure any device used for CWS-CARES access is properly secured.
4. Understand that all system activity is logged, monitored, and subject to audits.
5. Violations may result in revoked access, disciplinary measures, or legal consequences per CDSS and State of California policies.
6. By accessing the CWS-CARES system, users agree to this AUP, the Privacy Policy and the Condition of Use.