Staff OS — Data Protection Policy

Last Updated: February 10, 2026

---

1. INTRODUCTION

Staff OS, LLC ("Staff OS," "we," "us," or "our") operates an AI-powered recruitment engagement platform that processes personal information on behalf of our clients and in the course of our own business operations. This Data Protection Policy describes our approach to safeguarding personal information across our US and Canadian operations, with particular attention to the unique data protection considerations arising from AI-driven recruitment technology.

This policy should be read alongside our Privacy Policy, Terms of Service, and Data Processing Addendum (DPA).

---

2. SCOPE

This policy applies to all personal information processed by Staff OS, including:

- Candidate Data collected through AI conversations, screening processes, and database management
- Client personnel data associated with platform administration and billing
- Lead attribution and recruitment analytics data
- Data transferred between the United States and Canada in the course of service delivery
- Data received from integrated third-party platforms (e.g., Indeed, LinkedIn, client ATS systems)

---

3. DATA PROTECTION PRINCIPLES

Staff OS adheres to the following principles when processing personal information:

3.1 Lawfulness, Fairness, and Transparency. We process personal information on a lawful basis, treat individuals fairly, and are transparent about how their data is used—including informing candidates when they are interacting with an AI system.

3.2 Purpose Limitation. Personal information is collected for specified, legitimate recruitment and platform operation purposes and not further processed in a manner incompatible with those purposes, except where de-identified or aggregated for product improvement.

3.3 Data Minimization. We collect only the personal information reasonably necessary for the purposes for which it is processed. AI screening and conversation flows are designed to gather relevant recruitment information without requesting unnecessary personal details.

3.4 Accuracy. We take reasonable steps to ensure personal information is accurate and up to date. Clients and candidates may request corrections through established channels.

3.5 Storage Limitation. Personal information is retained only for as long as necessary to fulfill the applicable purpose, comply with legal obligations, or as specified in client agreements.

3.6 Integrity and Confidentiality. We implement appropriate technical and organizational measures to protect personal information against unauthorized access, loss, destruction, or damage.

3.7 Accountability. We maintain documentation and processes to demonstrate compliance with applicable data protection requirements.

---

4. LEGAL BASES AND REGULATORY FRAMEWORK

4.1 United States

Staff OS complies with applicable US federal and state privacy and data protection laws, including:

- **State Privacy Laws:** California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA), and other applicable state privacy statutes
- **Communications Laws:** Telephone Consumer Protection Act (TCPA), CAN-SPAM Act
- **Employment-Related Laws:** Equal Employment Opportunity Commission (EEOC) guidelines, state and local fair employment practices laws relevant to automated decision-making
- **Sector-Specific Laws:** FERPA (where education records may be relevant), and applicable state biometric information laws

4.2 Canada

Staff OS complies with Canadian privacy legislation, including:

- **PIPEDA** (Personal Information Protection and Electronic Documents Act)
- **Provincial Privacy Laws:** Alberta's PIPA, British Columbia's PIPA, and Québec's Law 25 (Act Respecting the Protection of Personal Information in the Private Sector), as applicable
- **CASL** (Canada's Anti-Spam Legislation) for electronic messaging
- **Provincial Employment Standards** relevant to automated recruitment processes

4.3 Consent Framework

We rely on the following bases for processing:

- **Consent:** Where required by law, we obtain informed consent before processing personal information, particularly for SMS/MMS messaging, AI-driven conversations, and database reactivation of dormant candidates. Consent mechanisms are designed to be clear, specific, and easily revocable.
- **Contractual Necessity:** Processing necessary to perform our contractual obligations to Clients.

- **Legitimate Interests:** Processing necessary for legitimate recruitment and platform improvement purposes, balanced against individuals' privacy interests.

---

5. AI-SPECIFIC DATA PROTECTION MEASURES

5.1 Transparency

- Candidates are informed when they are interacting with an automated AI system
- Clients receive documentation describing AI processing logic, screening criteria, and output formats
- This Data Protection Policy and our Privacy Policy describe AI data processing activities

5.2 Human Oversight

- AI-generated screening results and candidate assessments are presented as decision-support tools, not final determinations
- Our Terms of Service require Clients to ensure meaningful human oversight of employment decisions informed by AI outputs
- Candidates may request human review of AI-generated assessments

5.3 Bias Mitigation

- Staff OS conducts periodic reviews of AI model outputs to identify and mitigate potential bias
- Screening algorithms are configurable by Clients and are based on job-relevant criteria
- We maintain internal documentation of AI model development, testing, and evaluation processes

5.4 Data Used for AI Training

- AI models may be improved using de-identified and aggregated data only
- No individually identifiable personal information is used to train general-purpose AI models without appropriate de-identification
- Client Data used for model improvement is processed in accordance with the applicable DPA and Agreement

5.5 Bilingual Processing Safeguards

- AI processing in English and Spanish is subject to the same data protection standards
- Language preferences are respected and not used as a basis for differential treatment in screening or matching
- Translation and language detection logs are treated as part of conversation data and subject to the same retention and security policies

6. DATA HANDLING — SPECIFIC CATEGORIES

6.1 Recruitment Analytics and Lead Attribution

- Lead attribution data (e.g., source platform, campaign identifiers, conversion metrics) is collected to measure recruitment funnel performance
- Analytics data is associated with Client accounts and used for reporting and optimization
- Where analytics data includes personal identifiers, it is subject to the same protections as other personal information
- De-identified analytics may be used for benchmarking and product development

6.2 Real-Time Conversation Data

- AI conversations are processed in real time and stored as part of candidate records
- Conversation content is accessible to authorized Client personnel through the platform
- Conversation metadata (timestamps, response times, engagement metrics) is used for quality assurance and platform optimization
- Clients are responsible for ensuring that conversation data is handled in accordance with their own privacy obligations

6.3 Database Reactivation Data

- When Clients use database reactivation features, previously collected candidate data is re-processed for the purpose of re-engagement
- Staff OS requires Clients to confirm that valid consent exists before initiating reactivation campaigns
- Reactivation communications include opt-out mechanisms
- Candidates who have previously opted out are excluded from reactivation campaigns (based on data provided by the Client)

6.4 Cross-Platform Integration Data

- Data received from or transmitted to third-party platforms (e.g., Indeed, LinkedIn, client ATS/HRIS systems) is processed in accordance with this policy and the applicable DPA
- Clients are responsible for ensuring that data shared through integrations complies with the terms of the third-party platforms and Applicable Law

7. CROSS-BORDER DATA TRANSFERS

7.1 US-Canada Transfers

Staff OS operates across the United States and Canada. Personal information may be transferred between these jurisdictions in connection with service delivery. We implement the following safeguards:

- Contractual data protection clauses in our DPA and client agreements
- Technical safeguards including encryption in transit and at rest
- Access controls limiting data access to authorized personnel with a legitimate need
- Compliance with PIPEDA cross-border transfer requirements, including ensuring that transferred data receives a comparable level of protection

7.2 Sub-Processor Management

- We maintain a list of sub-processors who may access personal information
- Sub-processors are subject to contractual obligations at least as protective as those in our DPA
- Clients are notified of material changes to sub-processor arrangements in accordance with the DPA
- Sub-processor compliance is reviewed periodically

7.3 Data Localization

Unless specific data residency commitments are made in a Client's Order Form, Staff OS does not guarantee storage in a specific jurisdiction. Clients with data localization requirements should contact us prior to onboarding.

---

8. SECURITY MEASURES

8.1 Technical Safeguards

- Encryption of personal information in transit (TLS 1.2+) and at rest (AES-256 or equivalent)
- Multi-factor authentication for platform access
- Role-based access controls
- Network segmentation and firewalls
- Automated intrusion detection and monitoring systems
- Regular vulnerability scanning and penetration testing

8.2 Organizational Safeguards

- Written information security policies and procedures
- Employee background checks for personnel with access to personal information
- Regular security awareness training

- Incident response plans and procedures
- Business continuity and disaster recovery planning

8.3 Standards and Certifications

Staff OS maintains compliance with SOC 2 Type II and aligns with ISO 27001 standards. Compliance reports are available to Clients upon written request, subject to confidentiality obligations.

8.4 Incident Response

In the event of a data breach or security incident involving personal information:

- Staff OS will promptly investigate and contain the incident
- Affected Clients will be notified without undue delay and within the timeframes required by Applicable Law
- Staff OS will cooperate with Clients in meeting their own notification obligations
- Post-incident reviews will be conducted to identify and implement preventive measures

---

9. DATA SUBJECT RIGHTS

9.1 Rights Available

Depending on jurisdiction, individuals may exercise the following rights:

- **Access:** Obtain a copy of personal information held about them
- **Correction:** Request correction of inaccurate or incomplete data
- **Deletion:** Request erasure of personal information (subject to legal retention requirements)
- **Portability:** Receive personal information in a structured, commonly used format
- **Restriction:** Request restriction of certain processing activities
- **Objection:** Object to processing based on legitimate interests, including AI profiling
- **Withdrawal of Consent:** Withdraw previously given consent at any time
- **Human Review of AI Decisions:** Request that AI-generated screening or assessment results be reviewed by a human being

9.2 How to Exercise Rights

- Candidates may contact privacy@staff-os.com or the Client organization directly
- Where Staff OS processes data on behalf of a Client (as a processor/service provider), we will refer requests to the Client unless we can reasonably fulfill the request directly
- Requests will be responded to within the timeframes required by Applicable Law

9.3 Verification

We may verify the identity of individuals submitting requests to prevent unauthorized access to personal information.

---

10. THIRD-PARTY DATA SHARING AND ONWARD TRANSFERS

Staff OS shares personal information with third parties only as described in our Privacy Policy and subject to appropriate contractual and technical safeguards. Categories of recipients include:

- Cloud infrastructure and hosting providers
- Messaging and telecommunications carriers
- Analytics and monitoring tools
- Integrated third-party platforms designated by Clients
- Professional advisors (legal, audit, accounting)
- Government authorities where required by law

All third-party recipients are contractually obligated to protect personal information and limit its use to the purposes for which it was shared.

---

11. RETENTION AND DISPOSAL

11.1 Retention Schedule

Data Category	Retention Period
Active Candidate Data	Duration of Client subscription + 30 days
Dormant Candidate Data	Per Client instructions and applicable consent parameters
AI Conversation Logs	Duration of Client subscription + 30 days
Lead Attribution / Analytics	Duration of Client subscription; de-identified data may be retained indefinitely
Client Account / Billing Data	As required by tax and accounting laws (typically 7 years)
Security Logs	Minimum 12 months; longer where required for investigation
De-Identified / Aggregated Data	Indefinite

11.2 Disposal

Upon expiration of applicable retention periods or Client termination, personal information is securely deleted or de-identified using industry-standard methods. Deletion is confirmed upon Client request.

12. TRAINING AND AWARENESS

All Staff OS personnel with access to personal information receive training on:

- Data protection principles and obligations
- AI ethics and responsible use
- Security awareness and incident response
- Cross-border data transfer requirements
- Handling of data subject requests

Training is conducted at onboarding and refreshed annually, with additional training provided when material changes occur in data protection requirements or platform capabilities.

---

13. GOVERNANCE AND ACCOUNTABILITY

13.1 Data Protection Lead

Staff OS designates an internal data protection lead responsible for overseeing compliance with this policy and applicable data protection laws. Inquiries may be directed to privacy@staffos.com.

13.2 Records of Processing Activities

We maintain records of processing activities in accordance with Applicable Law, documenting the categories of data processed, purposes, recipients, retention periods, and security measures.

13.3 Data Protection Impact Assessments

Where required by Applicable Law or where processing presents a high risk to individuals' rights (including introduction of new AI capabilities or significant changes to screening algorithms), Staff OS conducts data protection impact assessments.

13.4 Policy Review

This policy is reviewed at least annually and updated as necessary to reflect changes in Applicable Law, platform capabilities, and business operations.

---

14. CONTACT

For questions or concerns about this Data Protection Policy, please contact:

- **Email:** privacy@staffos.com
- **Mail:** Staff OS, LLC, [Address], [City, State, ZIP]

This Data Protection Policy is provided for informational purposes and should be reviewed by qualified legal counsel before publication.