Creative Graphics Group

Cybersecurity and Data Privacy Policy

Review Date	Version	Reviewed by	Approved by
22nd April 2026	1.0	Senior Management	Board of Directors

Table of Contents

Purpose and Scope

Creative Graphics ('the Company') is committed to protecting the privacy, confidentiality, and integrity of Personal Information and Sensitive Personal Data or Information (SPDI), safeguarding its information systems and cybersecurity posture, and protecting the Company's and its clients' creative assets and intellectual property. This Policy governs the collection, processing, storage, transfer, retention, and disposal of personal data; cybersecurity practices and incident response; and the ownership, licensing, and confidentiality of creative work product. It is binding upon all employees, contractors, vendors, and third parties acting on behalf of the Company.

Objectives

This Policy aims to:

- Ensure lawful, fair, and transparent processing of all Personal Information and SPDI collected by the Company;
- Establish clear accountability through designated data protection responsibilities;
- Safeguard the rights of Data Principals, including rights to access, correction, erasure, and withdrawal of consent;
- Prevent unauthorised access, disclosure, alteration, or destruction of personal data;
- Ensure compliance with the Digital Personal Data Protection Act, 2023, the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and the Information Technology Act, 2000;
- Define clear retention periods and ensure secure disposal of data upon fulfilment of purpose;
- Establish a responsive grievance redressal mechanism for Data Principals; and
- Build a culture of data privacy awareness among all employees and stakeholders of the Company.

Collection of Personal Information

The Company collects Personal Information and SPDI only to the extent necessary for legitimate business or regulatory purposes. Consent shall be obtained explicitly from the Information Provider prior to collection of SPDI. Under the DPDPA 2023, consent is required prior to processing any personal data. Data is collected through employee onboarding, client and vendor engagements, and project exchanges. Consent is obtained through written forms during employee onboarding, email confirmations for client and vendor engagements, and digital acknowledgements where applicable. The Head - Human Resources (Head HR) is

responsible for overseeing grievance redressal in relation to personal data processing and shall maintain consent records in accordance with the Company's Data Retention Schedule.

Use and Processing of Personal Information

The Company shall process Personal Information and SPDI exclusively for legitimate, specified purposes, including HR administration, delivery of design and production services, client and vendor management, statutory compliance, and fraud prevention. The Company applies data minimisation principles. All personnel handling data are bound by confidentiality obligations. Data shall not be retained beyond the period necessary for its purpose or as mandated by law.

Disclosure and Transfer of Sensitive Personal Data or Information

The Company may disclose or transfer SPDI to authorised service providers, professional advisors, and Indian affiliates under contractual obligations, solely to the extent necessary. Disclosure may occur where mandated by law, court order, or government authority, or to prevent fraud. In the event of a corporate restructuring or asset sale, data may be transferred to the succeeding entity under equivalent obligations. All Third Parties receiving data shall execute NDAs confirming confidentiality and compliance with applicable law. Where any third-party vendor or service provider processes personal data on behalf of the Company, they shall be bound by a written agreement mandating processing only on the Company's instructions and in compliance with applicable data protection law.

Rights of the Information Provider

Under the DPDPA 2023, the following rights apply to all personal data held by the Company:

- **Right to Access and Correction:** An Information Provider may write to the Head HR to access or request correction of their data.
- **Right to Withdraw Consent:** An Information Provider may withdraw consent by written communication to chro@creativegraphics.net.in. Withdrawal operates prospectively and may result in discontinuation of services requiring that data. Data Principals may also manage or withdraw their consent through a registered Consent Manager, as provided under the DPDPA 2023.
- **Right to Nominate:** An Information Provider may nominate another individual to exercise their rights in the event of death or incapacity (DPDPA 2023, Section 14).
- **Right to Non-Discrimination:** The Company shall not subject any Information Provider to adverse treatment for exercising their rights.

- **Right to Erasure:** An Information Provider may request erasure where the purpose has been fulfilled, consent has been withdrawn, or data has been processed unlawfully. Valid requests shall be actioned within 30 days.
- **Right to Escalation:** A dissatisfied Data Principal may refer the matter to the Data Protection Board of India (DPDPA 2023, Section 27).

Cybersecurity Practices and Procedures

The Company is committed to ensuring the confidentiality, integrity, and availability of all data across its full lifecycle. We implement a robust framework of technical and organizational measures to safeguard data against unauthorized access, alteration, disclosure, or destruction.

Data Privacy and Information Security

To protect personal data and Sensitive Personal Data or Information (SPDI), the Company implements standard security controls, including:

- Access Control: Limiting data access to authorized personnel through role-based permissions and secure user authentication protocols.
- Network Security: Utilization of standard security tools, such as firewalls and anti-malware solutions, to protect server infrastructure.
- Vulnerability Management: Conducting periodic checks to identify and address potential security gaps.
- Confidentiality: Enforcing strict confidentiality obligations for all employees and contractors with access to sensitive data.
- Security Awareness: Ensuring all personnel handling personal data are informed of their security responsibilities upon onboarding and through ongoing updates.

Creative Asset, Intellectual Property, and Licensing

Client-provided design assets, artwork, and print-ready files are strictly protected. Access is limited to authorized personnel on a need-to-know basis. Work-in-progress files are stored securely and retained only for necessary operational periods. Third-party vendors must execute NDAs before accessing client assets. Client deliverables will never be shared publicly without prior written consent.

Ownership of Creative Output and Source Files

All original designs, layouts, illustrations, and concepts developed by the Company remain its intellectual property. Unless agreed otherwise in writing, full payment transfers ownership of final flattened deliverables (e.g., JPEG, PNG, PDF and other similar file formats) only. Layered source files and raw working project files (e.g., PSD, AI, INDD and other similar file formats) remain the sole property of the Company and require a separate buyout fee to transfer.

Artificial Intelligence (AI) and Machine Learning

The Company guarantees that all primary creative concepts and final designs feature human authorship. If Generative AI tools (e.g., Adobe Firefly, Midjourney and other similar AI tools) are utilized for brainstorming or asset generation, the Company ensures strict compliance with commercial licensing terms to safeguard the client's commercial utility and intellectual property rights.

Client-Provided Materials

Logos, brand assets, product images, and text supplied by the client remain their exclusive intellectual property. The Company shall use these materials solely to execute the commissioned work. Employees and external vendors must handle client-owned assets securely and strictly within the assigned project scope.

Third-Party Licensed Content

The Company ensures valid commercial licensing for all third-party stock imagery, fonts, and design templates incorporated into deliverables. Licenses will strictly match the client's intended commercial and geographic distribution. The Company maintains comprehensive licensing records and communicates any applicable license costs to the client in advance.

Confidentiality of Unreleased Work

Unreleased designs, concepts, packaging mock-ups, and pre-press proofs are confidential. They must not be shared externally including on social media, in professional portfolios, or with other clients-without explicit written client consent. The Company will obtain written permission before featuring completed work in its promotional materials.

Employee and Contractor Obligations

All rights, titles, and intellectual property in any creative work produced by employees and contractors during their engagement belong exclusively to the Company from the moment of creation. Team members are prohibited from copying, repurposing, or claiming personal ownership of any project files. Upon separation, all source files and design assets must be returned or permanently deleted from personal devices. Violations will result in disciplinary action and legal recourse under the Copyright Act, 1957.

Grievance Redressal & Retention

Any grievances concerning the processing of Personal Information or SPDI shall be directed in writing to the Head HR, who is responsible for grievance redressal under this Policy, at chro@creativegraphics.net.in

The Head HR shall acknowledge receipt of any grievance within 48 hours and resolve all grievances within 30 days, in accordance with the Digital Personal Data Protection Act, 2023.

Document retention periods applicable to the Company's records shall be managed by the respective departments responsible for maintaining such records, in accordance with applicable legal, regulatory, contractual, and business requirements. Key retention periods applicable to the Company's operations are as follows:

- Employee personal and HR records: 8 years from end of employment;
- Client project files and creative assets: as specified in contract, or 3 years from project completion;
- Consent records: duration of the relationship with the Data Principal plus 3 years thereafter.
- Financial and invoicing records: 7 years (Companies Act, 2013);
- Incident and breach records: 5 years;
- ICT system and security logs: 180 days (CERT-In requirements).

Incident Response Plan

Upon detection of a cybersecurity incident or personal data breach, the Company's designated management lead shall immediately isolate affected networks or cloud-based print folders, secure all access logs, and notify corporate clients whose data may be impacted. Qualifying cybersecurity incidents must be reported to the Indian Computer Emergency Response Team (CERT-In) via incident@cert-in.org.in within 6 hours of discovery, in accordance with the CERT-In Directions. For incidents involving a personal data breach (such as leaked customer files or print logs), the Company shall execute the two-stage reporting framework under Rule 7 of the DPDP Rules: providing an initial notification without delay simultaneously to the Data Protection Board of India (DPBI) and affected individuals, followed by a comprehensive, detailed report submitted to the DPBI within 72 hours of becoming aware of the breach. To ensure compliance, all digital ICT and data processing logs must be securely archived within Indian servers for at least 1 year, and a formal record of the incident must be maintained in the Company's internal Incident Register for a minimum of 5 years.

Processing of Children's Personal Data

The Company does not knowingly collect, process, or store children's personal data, as its services in graphics, printing, packaging, and design are directed exclusively at businesses and adult individuals. If such data is inadvertently received, the Company shall promptly delete it, notify the parent or lawful guardian where practicable, and review and strengthen the relevant intake processes. Should future business activities involve processing children's personal data, this Policy will be updated to incorporate verifiable parental consent mechanisms and all safeguards mandated under Section 9 of the Digital Personal Data Protection Act, 2023 prior to such processing.

Changes to this Policy

This Policy shall be reviewed periodically, or earlier if required by changes in applicable laws, regulations, or business operations. The Head HR shall oversee the implementation and review of the Policy and ensure that it remains current and effective. Any approved revisions shall be communicated through appropriate internal or external channels, as applicable.

ANNEXURE

Annexure I - Definitions

- **Personal Information:** Any data relating to a natural person that, directly or indirectly, is capable of identifying that individual.
- **Sensitive Personal Data or Information (SPDI):** A sub-category of Personal Information warranting heightened protection - including passwords, financial data, health information, biometric data, and confidential creative assets.
- For the purposes of the DPDPA 2023, all Personal Information collected by the Company - irrespective of whether it constitutes SPDI - is treated as personal data and afforded the full protection standards prescribed under that Act. The SPDI classification is maintained for internal data security tiering compliance purposes.
- **Information Provider:** Any individual - employee, client, vendor, contractor, or website user - who provides Personal Information or SPDI to the Company.
- **Child:** A person who has not completed eighteen years of age (per DPDPA 2023, Section 2(c)).
- **Third Party:** Any entity outside the Company that receives or has access to data held by the Company.
- **Data Fiduciary / Data Principal:** Carry the meanings under the DPDPA 2023. The Company is the Data Fiduciary; the individual whose data is processed is the Data Principal.

Annexure II - Standards Referred

- Information Technology Act, 2000
- IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Digital Personal Data Protection Act, 2023 (India)

****