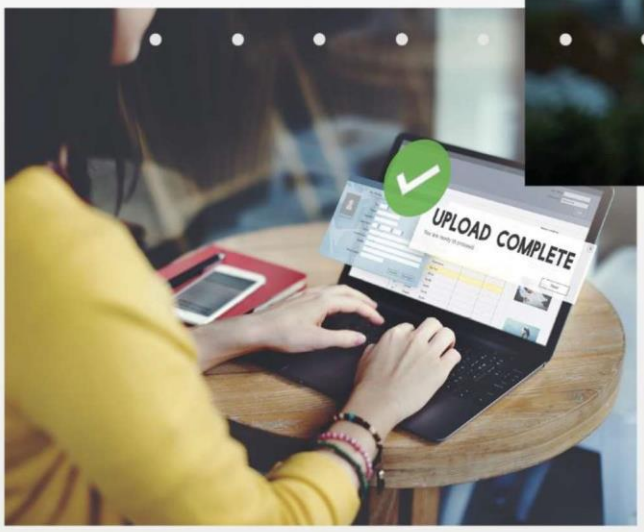
APOGEE
An HP Company



Privacy Policy
October 2024

For more information, visit
apogeecorp.com

1. Definitions and Abbreviations

Apogee	Collectively refers to Apogee Corporation Limited and all of its subsidiaries and affiliates.
Data	Any information which is stored or otherwise processed in any format by Apogee staff or automated systems.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
Data Controller (or controller)	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor (or processor)	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Data Protection Officer (DPO)	The named person within the business who is overall responsible for the oversight and implementation of GDPR and acts as a point of contact for the data subjects.
Data Protection Impact Assessment (DPIA)	A process to assess the impact of high-risk processing activities on individuals' privacy.
Data Subject	A natural person whose personal data is processed by Apogee.
Data Users	Employees whose work involves using personal data.
EEA	The European Economic Area, comprising the member states of the European Union plus Iceland, Liechtenstein, and Norway.
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access.
International Data Transfer	The transfer of personal data to a country outside the UK or EEA.

General Data Protection Regulation (GDPR):	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Legal Person	A legal entity or organisation
Natural Person	A human being, as opposed to a legal person.
Personal Data:	Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Special Categories of Personal Data (or Sensitive Personal Data)	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, or data concerning a natural person's sex life or sexual orientation.
Third Party	Any external organization or individual that Apogee shares personal data with.

UK GDPR	The UK General Data Protection Regulation, which is the UK's implementation of the GDPR following its departure from the European Union.

2. Introduction

At Apogee, we value our customers and understand that protecting the information you entrust us with is paramount. We are committed to respecting your privacy and handling your data responsibly and transparently, in full compliance with all applicable data protection laws.

This Privacy Policy outlines how we collect, use, share, and safeguard your personal information when you interact with Apogee, use our services, visit our websites, or become part of our team. Please take a moment to read this policy carefully as it contains important information about:

- **What personal data we collect about you:** This includes information like your name, contact details, and depending on your relationship with us, additional data relevant to our services or your employment.
- **How we collect your personal data:** We gather information through various channels, such as when you use our services, visit our websites, contact us, or apply for a job.
- **What we use your personal data for:** We use your information to provide our services, manage our business operations, communicate with you, and comply with legal obligations.
- **When we may share your personal data**: We may share your information with trusted third parties who assist us in providing our services or as required by law.
- **How we protect your personal data:** We have robust security measures in place to safeguard your information.
- **Your rights in relation to your personal data:** You have the right to access, correct, and control your personal data in accordance with applicable laws.

This policy applies to the information we collect while:

- Providing our IT services, digital workplace solutions, managed print services, and outsourced document services.
- Interacting with you as a customer, client, or potential client.
- Communicating with you through our websites, emails, or other channels.
- Engaging with you as an employee, contractor, or job applicant.
- Operating our business, including managing our internal systems and security.

By understanding this policy, you can make informed decisions about sharing your personal information with us and feel confident that your data is handled responsibly.

If you have any questions or concerns about our privacy practices, please do not hesitate to contact us.

3. About Apogee

Apogee (referred to as "Apogee," "we," "us," or "our" in this policy) is a leading provider of managed IT services, digital workplace solutions, managed print services, and outsourced document services. We operate primarily in the UK, with additional operations in Ireland, Isle of Man, Jersey, France, and Germany. Apogee owns and operates this website and a number of others, including:

- Apogee:
    - https://apogeecorp.com/
    - https://www.apogeegraphics.co.uk/
- Argon: https://www.argon.im/
- Datatron: https://www.datatron.co.uk/

This Privacy Policy applies to all entities within the Apogee Group that process personal data.

4. What Personal Data We Collect

The specific personal data we collect depends on your relationship with Apogee. We've categorised the types of data we might collect as follows:

4.1. Customers and Clients

- **Contact Information:** Name, business address, email address, phone number, job title, and department.
- **Service-Related Information:** Information relating to the specific services you or your company receive from Apogee, including service requests, usage data, and any other information necessary to provide and support our services.
- **Billing and Financial Information:** Invoicing details, payment information, and any other financial data necessary for processing transactions.
- **Communication Data:** Records of any interactions with our customer support team, including phone calls, emails, or chat transcripts.
- **Device and Network Information:** If we provide IT or digital workplace solutions, we may collect information about your devices, networks, IP address, or systems to ensure proper functionality and security.

If you use our outsourced document services, we may also collect we may also collect and process document content, delivery addresses, and mailing preferences to provide our outsourced printing and mailing services, including mailroom post opening and Auto mail.

If you use our technical IT services, we may also collect technical data related to your IT systems, networks, and devices, as well as data related to managed print solutions and cabling services.

4.2. Website Visitors

- **Technical Information:** IP address, browser type and version, operating system, referring website, pages visited, and time spent on our websites.
- **Cookies and Similar Technologies:** We use cookies and similar technologies to enhance your browsing experience and collect information about how you use our websites. Please see our Cookie Policy for more details.

4.3. Employees, Contractors, and Job Applicants

- **Personal Details:** Name, address, date of birth, contact information, emergency contact details, national insurance number, bank details, and other information necessary for payroll and HR purposes.
- **Employment Information:** Job title, department, employment history, qualifications, performance reviews, training records, and other relevant work-related information.
- **Identification and Background Check Information:** Copies of identification documents (e.g., passport, driver's license), background check results, and other information necessary for compliance and security purposes.
- **Access and Security Information:** Records of your access to our premises, systems, and networks, including CCTV footage and access logs.

4.4. Sensitive Personal Data

In certain limited circumstances, we may collect and process sensitive personal data, such as health information or data revealing racial or ethnic origin, only when it's strictly necessary for specific purposes and with your explicit consent or as permitted by law (e.g., for employment, social security, or vital interests). We implement additional safeguards to protect this sensitive information.

We may also process health-related data when necessary for business continuity and disaster recovery planning, with your explicit consent or as required by law.

Please note: This is not an exhaustive list and the specific personal data we collect may vary depending on the services you use or your relationship with Apogee.

5. How We Collect Your Personal Data

We collect personal data about you through various channels, including:

5.1. Directly from You

- **When you interact with us:** This includes when you:
  - Fill out forms or provide information on our websites or applications.
  - Contact us via phone, email, or in person.
  - Request information or quotes about our services.
  - Subscribe to our newsletters or marketing communications.
  - Apply for a job or become an employee or contractor.

- Visit our premises or attend our events.

5.2. Through Our Websites and Applications

- **Cookies and Similar Technologies:** We use cookies and other tracking technologies to collect information about your browsing behaviour and preferences. This helps us improve our websites, personalise your experience, and deliver relevant content. For more details, please refer to our Cookie Policy.
- **Web Server Logs:** Our web servers automatically collect certain technical information, such as your IP address, browser type, operating system, and referring website. This information is used for system administration, troubleshooting, and security purposes.

5.3. From Third Parties

- **Service Providers:** We may receive personal data from third-party service providers who assist us in delivering our services or conducting our business operations. These may include IT providers, marketing agencies, background check providers, credit reference agencies, and others.
- **Publicly Available Sources**: In some cases, we may collect personal data from publicly available sources, such as social media platforms, company websites, or Companies House, to verify information or for business development purposes.
- **Referrals:** We may collect personal data about you from individuals who refer you to us for our services or employment opportunities.

5.4. Automated Decision-Making and Profiling

In certain circumstances, we may use automated decision-making processes, including profiling, to personalise our services, tailor marketing communications, or assess your suitability for employment. We will always inform you when such processes are used and provide you with the opportunity to object or request human intervention.

6. What We Use Your Personal Data For

We use your personal data for various purposes, depending on your relationship with us. These purposes include:

6.1. Customers and Clients

- **Providing and Managing Services:** To fulfil our contractual obligations and provide the IT services, digital workplace solutions, managed print services, or outsourced document services you have requested. This includes:

  - Processing service requests and orders
  - Delivering and managing services
  - Providing technical support and troubleshooting
  - Billing and invoicing
  - Communicating with you about your account and services

- Processing and managing documents for printing, mailing, and other outsourced document services.
- Receiving, opening, scanning, filing, and sharing client post as part of our mailroom services.
- Designing, implementing, supporting, and maintaining IT systems, including PC, server, data centre, and cloud solutions.
- Providing managed print solutions, including multi-functional devices, printers, and mailroom products.
- Delivering cabling services, including surveys, design, installation, and testing.
- Offering business continuity and disaster recovery services, including access to our resilient facilities and on-site data centre.

- **Business Operations and Communication:** To manage our relationship with you and your company, including:

  - Responding to inquiries and requests
  - Sending important service updates and notifications
  - Conducting customer satisfaction surveys
  - Managing and improving our services

- **Contract and Account Management:** To manage our contractual relationship with you, including handling inquiries, processing orders, managing your account, and providing customer support.

- **Marketing and Sales:** With your consent, we may use your personal data for marketing and sales purposes, such as:

  - Sending you promotional offers and newsletters
  - Inviting you to events or webinars
  - Conducting market research and analysis

- **Legal and Regulatory Compliance:** To comply with our legal and regulatory obligations, such as:

  - Preventing and detecting fraud
  - Conducting due diligence checks
  - Responding to legal requests and court orders

Legal Basis for Processing: The legal basis for processing your personal data in relation to our services is primarily the performance of a contract. We may also rely on legitimate interests for certain processing activities, such as improving our services and communicating with you about relevant offerings. We may also process your data based on your consent, particularly for certain marketing activities.

6.2. Website Visitors

- Improving our websites: To analyse website usage and improve our website's functionality and content.
- Personalising your Experience: To tailor the content and advertisements you see on our websites based on your interests and preferences.
- Communicating with you: To respond to your inquiries or provide information you request.

Legal Basis for Processing: We rely on legitimate interests to process your data for website analytics and improvement purposes. For personalised advertising and *direct* marketing communications, we will obtain your consent.

6.3. Employees, Contractors, and Job Applicants

- Recruitment and Onboarding: To process job applications, conduct interviews, and onboard new hires.
- Human Resources Management: To manage employee records, payroll, benefits, performance evaluations, training, and other HR-related activities.
- Workplace Management and Security: To manage access to our premises and systems, ensure workplace safety, and protect our assets.
- Internal Communication and Collaboration: To facilitate communication and collaboration among our employees and contractors.

Legal Basis for Processing: The legal basis for processing your personal data in relation to your employment or application is primarily the performance of a contract or compliance with legal obligations. We may also rely on legitimate interests for certain processing activities, such as managing employee performance and maintaining a safe workplace. We may also process your data to protect your vital interests or those of another person, particularly in emergency situations where we need to process health data for your well-being.

6.4. International Data Transfers

In some cases, we may need to transfer your personal data to countries outside the European Economic Area (EEA) where data protection laws may not be as stringent. When we do so, we will ensure appropriate safeguards are in place to protect your data, such as using Standard Contractual Clauses approved by the European Commission or relying on other valid transfer mechanisms.

7. When We May Share Your Personal Data

We understand the importance of safeguarding your personal data and will only share it when necessary for legitimate business purposes or as required by law. We may share your personal data with the following categories of recipients:

7.1. Within the Apogee Group

We may share your personal data with other companies within the Apogee Group for internal administrative and operational purposes, such as providing centralised IT support, managing customer relationships, or conducting group-wide marketing activities.

7.2. Third-Party Service Providers

We may engage trusted third-party service providers to assist us in delivering our services or conducting our business operations. These service providers may have access to your personal data only to the extent necessary to perform their functions on our behalf and are contractually obligated to maintain its confidentiality and security. Examples of such service providers include:

- **IT and Cloud Service Providers:** To host and manage our IT systems, applications, and data.
- **Marketing and Communication Platforms:** To send you marketing communications, manage email campaigns, and analyse campaign performance.
- **Payment Processors:** To securely process payments for our services.
- **Background Check Providers:** To conduct background checks on job applicants and employees, where permitted by law.
- **Professional Advisors:** Such as lawyers, accountants, and auditors, to provide professional advice and services.

7.3. Other Third Parties

We may also share your personal data with other third parties under the following circumstances:

- **With Your Consent:** We may share your personal data with third parties when you have given us your explicit consent to do so.
- **Legal and Regulatory Requirements:** We may disclose your personal data if required to do so by law, regulation, court order, or other legal process.
- **Business Transfers:** In the event of a merger, acquisition, or sale of all or part of our business, your personal data may be transferred to the new owner or successor entity.
- **Law Enforcement and Government Agencies:** We may disclose your personal data to law enforcement or other government agencies when required by law or to prevent, investigate, or detect crime.

7.4. Sub-Processors

We may engage sub-processors to process personal data on our behalf.

- **Processors within the EEA or UK:** When we engage sub-processors located within the EEA or UK, we ensure they are contractually obligated to comply with applicable data protection laws and implement appropriate technical and organisational measures to protect your personal data.
- **Processors outside the EEA or UK:** If we engage sub-processors located outside the EEA or UK, we will ensure that appropriate safeguards are in place, such as Standard Contractual Clauses or other approved transfer mechanisms, to ensure your personal data is adequately protected.
- **Access to Information:** We are committed to transparency. If you have any questions or require a list of sub-processors engaged in holding your data and delivering services, please email the Apogee Legal Team at legal@apogeecorp.com.

We are committed to being transparent about our data sharing practices and providing you with choices where possible. You may have the right to object to or restrict certain types of data sharing. If you have any concerns or wish to exercise your rights, please contact our Legal Team at legal@apogeecorp.com. You can also opt out of receiving marketing communications by clicking the '**unsubscribe**' link in any marketing email or by contacting us directly.

8. How We Protect Your Personal Data

At Apogee, we understand the importance of safeguarding your personal data and have implemented a robust security framework to protect it from unauthorised access, loss, alteration, or disclosure.

8.1. Security Measures

We employ a multi-layered approach to security, incorporating industry-standard technical and organisational measures, including:

- **Access Controls:** Strict access controls limit access to personal data to authorized personnel only, based on their job responsibilities and on a need-to-know basis.
- **Encryption:** We use encryption technologies to protect sensitive data both at rest and in transit.
- **Network Security:** Our networks are protected by firewalls and intrusion detection systems to prevent unauthorized access and malicious activity.
- **Physical Security:** We maintain physical security measures at our facilities to prevent unauthorized access to our data centres and storage areas.
- **Employee Training and Awareness:** We provide regular training and awareness programs to our employees on data protection best practices and the importance of maintaining data confidentiality.

8.2. Data Storage and Transfers

Your personal data is primarily stored within secure data centres located within the European Economic Area (EEA). However, in some cases, we may need to transfer your data to countries outside the EEA, including to other Apogee Group entities or trusted third-party service providers. When we transfer data internationally, we ensure that appropriate safeguards are in place to protect your data, such as:

- **Standard Contractual Clauses (SCCs):** We implement SCCs approved by the European Commission to ensure adequate protection for data transferred outside the EEA. These clauses establish contractual obligations on the data recipient to protect your personal data.
- **Other Approved Transfer Mechanisms:** Depending on the specific circumstances, we may also rely on other approved transfer mechanisms, such as Binding Corporate Rules (BCRs) which are internal data protection policies approved by EU data protection authorities, or other mechanisms recognized under the UK GDPR or applicable laws.

8.3. Data Retention

We retain your personal data only for as long as necessary to fulfil the purposes outlined in this Privacy Policy or as required by law. We have established data retention schedules for different types of personal data, taking into account legal obligations, contractual requirements, and business needs. Once the retention period has expired, we will securely delete or anonymise your personal data.

9. Your Rights in Relation to Your Personal Data

You have certain rights regarding your personal data under applicable data protection laws. These rights include:

- **Right of Access:** You have the right to request a copy of the personal data we hold about you. This is often referred to as a **"subject access request."**
- **Right to Rectification:** You have the right to request that we correct any inaccurate or incomplete personal data we hold about you.
- **Right to Erasure:** In certain circumstances, you have the right to request that we erase your personal data. This is also known as the **"right to be forgotten."**
- **Right to Restriction of Processing:** You have the right to request that we restrict the processing of your personal data in certain situations.
- **Right to Data Portability:** You have the right to request that we provide you with your personal data in a structured, commonly used, and machine-readable format, or to transmit your data directly to another controller, where technically feasible.
- **Right to Object**: You have the right to object to the processing of your personal data in certain circumstances, particularly when we rely on legitimate interests as the legal basis for processing.

- **Right to Withdraw Consent:** If we rely on your consent to process your personal data, you have the right to withdraw that consent at any time.

9.1. How to Exercise Your Rights

To exercise any of these rights, please contact us using the contact details provided at the end of this Privacy Policy. We may need to verify your identity before fulfilling your request.

We aim to respond to your request within one month. In some cases, it may take longer, but we will notify you if this is the case. We may also need to request additional information from you to verify your identity before fulfilling your request.

9.2. Right to Lodge a Complaint

If you are not satisfied with how we handle your personal data or believe we are not complying with data protection laws, you have the right to lodge a complaint with the relevant supervisory authority.

- **United Kingdom:** The Information Commissioner's Office (ICO). You can find their contact details on the ICO website: https://ico.org.uk/..
- **Ireland:** The Data Protection Commission (DPC). You can find their contact details on the DPC website: https://www.dataprotection.ie/en..
- **Germany:** The relevant state data protection authority where you reside or where the alleged infringement occurred. You can find a list of the German state data protection authorities on the BfDI website (Federal Commissioner for Data Protection and Freedom of Information) https://www.bfdi.bund.de/DE/Service/Anschriften/anschriften_table.html..
- **France:** The Commission Nationale de l'Informatique et des Libertés (CNIL). You can find their contact details on the CNIL website https://www.cnil.fr/en/contact-us..
- **Jersey:** The Office of the Information Commissioner (OIC). You can find their contact details on the Jersey OIC website: https://jerseyoic.org/.
- **Isle of Man:** The Information Commissioner. You can find their contact details on the Isle of Man Government website https://www.gov.im/about-the-government/data-protection-gdpr-on-the-isle-of-man/data-protection-for-individuals/.

Please note that if you reside or the alleged infringement occurred in another jurisdiction where Apogee operates, you may also have the right to lodge a complaint with the corresponding supervisory authority in that jurisdiction.

10. How We Update or Change This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our data processing practices, legal requirements, or other operational factors. Any changes we make will be posted on this page, and the revised policy will include an updated effective date.

We will not significantly change how we use your personal data without providing you with clear notice and an opportunity to object.

For significant changes that may materially affect your rights or how we use your personal data, we will make reasonable efforts to notify you directly, such as through email or prominent notices on our website.

We encourage you to review this Privacy Policy periodically to stay informed about how we are protecting your information.

11. How You Can Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy, your personal data, or your data protection rights, please contact our Data Protection Officer (DPO) and Head of Legal, Robert Marr, using the following details:

- **Email:** legal@apogeecorp.com
- **Postal Address:** Nimbus House, Liphook Way, Maidstone, Kent, ME16 0FZ, UK

We are committed to addressing your inquiries and concerns promptly and effectively. Please do not hesitate to contact us if you have any questions or concerns about this Privacy Policy or how we handle your personal data.

Document Control

DOCUMENT NAME	VERSION	MASTER COPY LOCATION
Privacy Policy	2	Compliance SharePoint

Unless stated within the body of this document, the owner is responsible for maintaining document control and facilitating compliance, as well as the management of review, updates and changes.

OWNER	ROLE / ORGANISATION	CONTACT
Simon Green	Chief Information Officer	Simon.green@apogeecorp.com
AUTHOR	**ROLE**	**CONTACT**
Keith Harvey	Head of Compliance	Keith.harvey@apogeecorp.com

REVISION HISTORY

Version	Date	Amended By	Summary of changes
1	2020/01/06	Robert Marr/Simon Green	Original policy published on the website

2	2024/09/24	Keith Harvey	Updated the policy structure, clarified data collection and sharing practices, and enhanced user rights information to comply with current data protection regulations

DOCUMENT REVIEWS

This document has been reviewed for QC purposes by the following, in addition to those on the 'approvers' list.

Version	Date	Name	Title / Role
2		Robert Marr	DPO/Head of Legal
2		Simon Green	Chief Information Officer
2		Samantha Jackson	Chief Finance Officer
2		Marion Brooks	Chief People Officer
2		James Clark	Chief Executive Officer
2		Elia Giovanni	Director of Product & Go to Market
2		Dom Gryszan	Director of Marketing
2		Rachel Banks	Head of Product Management

APPROVALS

This document requires the following approvals for implementation and / or for any change in content.

Version	Date	Name	Title / Role	Approval Status (Pending/Approved)
2	2024-09-24	Simon Green	Chief Information Officer	Pending
2		James Clark	Chief Executive Officer	Pending