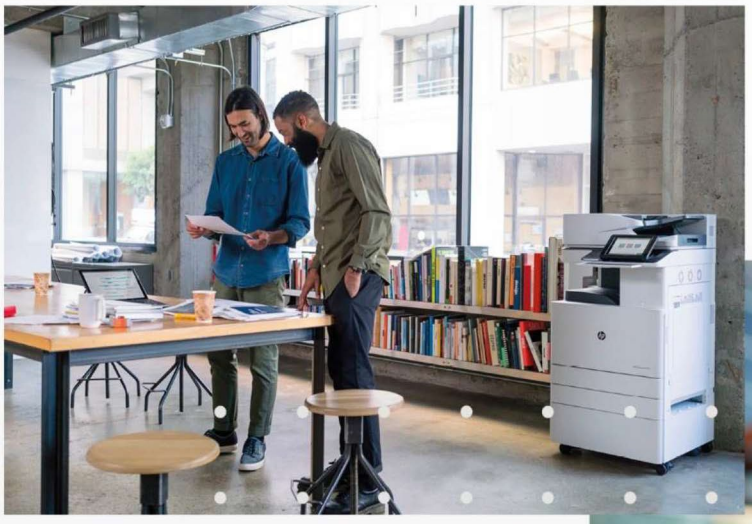
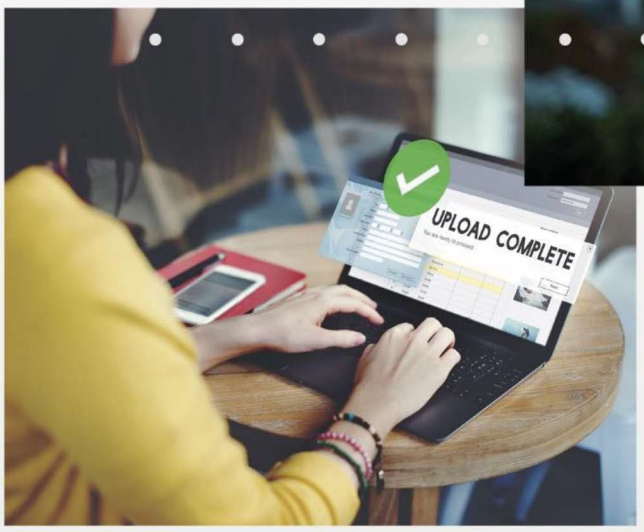
APOGEE
An HP Company





Data Protection Policy
September 2024

For more information, visit
apogeecorp.com

APOGEE
An HP Company

Contents

1. Definitions and Abbreviations

Apogee Corporation Limited (Apogee)	Refers to Apogee Corporation Limited and all 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 organisation 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

2.1. Purpose and Scope

This Data Protection Policy outlines Apogee's commitment to protecting the personal data of individuals we interact with, including employees, customers, partners, and other stakeholders. We recognise the importance of data privacy and individuals' rights under data protection laws.

This policy applies to all Apogee employees, contractors, consultants, temporary workers, and any other personnel who may access or process personal data on behalf of Apogee. It covers all personal data processed by Apogee, regardless of format or method.

The policy establishes a framework to ensure we collect, process, store, and share personal data lawfully, fairly, and transparently, prioritising the protection of individual privacy rights.

This policy is part of a broader data protection framework at Apogee. For specific guidance on data retention and data breaches, please refer to the Apogee Data Retention Policy and Data Breach Policy, respectively.

2.2. Legal Landscape

Apogee operates primarily within the United Kingdom and is therefore subject to the UK General Data Protection Regulation (UK GDPR) as its primary data protection jurisdiction. We are also committed to adhering to local interpretations and implementations of GDPR principles in regions where we have operations, including:

- Germany
- France
- Jersey
- Isle of Man
- Ireland

Apogee will maintain compliance with the strictest applicable data protection standards in each jurisdiction to ensure the consistent and robust protection of personal data.

2.3. Key Principles

This policy is guided by the following key data protection principles, which form the foundation of our approach to handling personal data:

- **Lawfulness, Fairness, and Transparency:** We will process personal data lawfully, fairly, and in a transparent manner. This means we will have a valid legal basis for all

processing activities, be open and honest with individuals about how we use their data and provide clear and accessible privacy notices.

- **Purpose Limitation:** We will collect personal data only for specified, explicit, and legitimate purposes. We will not further process data in a way that is incompatible with these original purposes.
- **Data Minimisation:** We will collect and process only the minimum amount of personal data necessary for the intended purposes. We will avoid collecting excessive or irrelevant data
- **Accuracy:** We will take reasonable steps to ensure personal data is accurate and kept up to date. We will establish procedures to rectify or erase inaccurate information promptly.
- **Storage Limitation:** We will retain personal data only for as long as necessary for the intended purposes. We will implement data retention policies and securely dispose of data when it is no longer needed.
- **Integrity and Confidentiality:** We will implement appropriate technical and organisational measures to ensure the security of personal data, protecting it from unauthorised access, loss, alteration, or destruction.
- **Accountability:** We will demonstrate compliance with data protection principles and be accountable for our data processing activities. This includes maintaining records of processing activities, conducting Data Protection Impact Assessments (DPIAs) when necessary, and cooperating with regulatory

3. Roles and Responsibilities

Roles	Responsibilities
Albacore (Apogee) Group Board	• Reviewing and overseeing Apogee's data protection framework and compliance with relevant regulatory requirements. • Receives regular reports on risk exposures and mitigation efforts.
Audit and Risk Committee	• **Oversight:** Pursuant to its terms of reference in effect from time to time, provides independent oversight of the risk management and compliance program on behalf of the Board. • **Risk Management:** Review and advise on data protection risks and mitigation strategies. • **Reporting:** Report to the Board on data protection compliance and any significant data protection incidents.
Chief Executive Officer (CEO):	• Responsible for the establishment, implementation and day-to-day management of the Data Protection program. • Ensures adequate resources are allocated to data protection management activities.

	• Reports to the Board on the effectiveness of the data protection framework • **Policy Approval:** Approve and oversee the implementation of this Data Protection Policy and any related procedures
The Executive Leadership	• **Strategic Direction:** Set the strategic direction for data protection within Apogee. • **Resource Allocation:** Ensure adequate resources are allocated to data protection compliance efforts. • **Culture of Compliance:** Foster a culture of data protection awareness and compliance throughout the organisation.
Data Security Group	• **Operational Implementation:** Implement and maintain technical and organizational measures to protect personal data. • **Security Incident Management:** Develop and implement incident response procedures for data breaches. • **Security Awareness:** Conduct regular security awareness training for employees.
Senior Management	• **Departmental Compliance:** Implements data protection by design and default principles in new projects and initiatives. Ensure that their departments comply with this Data Protection Policy and any related procedures. • **Data Processing Activities**: Conducts regular reviews of data processing activities within their departments. • **Employee Training:** Ensures their teams receive appropriate data protection training.
All Employees	• **Policy Adherence:** Comply with this Data Protection Policy and any related procedures. • **Data Handling**: Handle personal data in a responsible and secure manner. • **Incident Reporting:** Report any suspected data breaches or security incidents promptly.
Compliance Department	• **Policy Development and Review:** Develop, maintain, and review this Data Protection Policy and related procedures. • **Compliance Monitoring:** Monitor compliance with data protection laws and regulations. • **Data Protection Impact Assessments (DPIAs):** Conduct DPIAs for high-risk processing activities. • **Training and Awareness:** Develop and deliver data protection training and awareness programs. • **Advice and Guidance:** Provide advice and guidance on data protection matters to all employees.
Legal Department	• **Legal Advice:** Provide legal advice on data protection matters.

	• **Contractual Review:** Review contracts and agreements to ensure compliance with data protection laws. • **Litigation Support**: Provide support in the event of data protection-related litigation or regulatory investigations.
Data Protection Officer (DPO)	• Ensures Apogee's compliance with data protection laws and regulations. • Acts as the primary point of contact for data subjects and supervisory authorities. • Provides advice and guidance on data protection matters. • Monitors internal compliance. • **Contact details:** Robert Marr: legal@apogeecorp.com

4. Policy Requirements

4.1. Data Handling & Security

4.1.1. General Staff Guidelines:

4.1.1.1. **Data Sharing:** Personal data should only be shared with individuals who have a legitimate need to know, strictly in line with their work responsibilities.

4.1.1.2. **Formal Communication:** Avoid sharing data informally. When access is required, request it from line managers or data owners.

4.1.1.3. **Data Security:** Maintain data security by taking sensible precautions and following company guidelines:

- Use strong, unique passwords and never share them.
- Do not disclose personal data to unauthorized people, internally or externally.
- Regularly review and update data, deleting it securely when no longer required.
- Seek guidance from the Compliance Department if unsure about any aspect of data protection.
- Passwords must be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and symbols.
- Apogee shall employ strong encryption algorithms, currently at a minimum of AES-256 or its equivalent, to protect sensitive data both at rest (stored on devices or servers) and in transit (transmitted over networks). The specific encryption standards and protocols used may be updated periodically to reflect evolving best practices and technological advancements, as determined by the Data Security Group.
- Adhere to the Apogee Clean Desk Policy to ensure the physical security of data.

- When transferring personal data internationally, ensure appropriate safeguards are in place, such as Standard Contractual Clauses or Binding Corporate Rules. Obtain necessary consents for international transfers where required.

In addition to the security measures outlined in this policy, Apogee has implemented a range of technical and organizational controls to protect personal data. For more information, please refer to the Apogee Information Security Policy.

4.1.2. Data Storage

4.1.2.1. Paper-Based Data

- Store in locked drawers or filing cabinets when not in use.
- Do not leave paper or printouts where unauthorised people could see them.
- Shred or dispose of data printouts using confidential waste bins.

4.1.2.2. Electronic Data:

- Protect with strong passwords, changed regularly and not shared.
- Encrypt and store removable media securely.
- Store data only on designated drives and servers, or approved cloud storage services.
- Locate servers containing personal data in secure areas.
- Back up data frequently and test backups regularly.
- Never save data directly to unencrypted laptops or mobile devices.
- Protect all devices with approved security software and a firewall.
- Lock computer screens when unattended.
- Do not send personal data via email unless encrypted.
- Encrypt data before electronic transmission. Consult the Data Security Group for guidance on secure transfers.
- Do not transfer personal data outside the UK or EEA without authorisation. Consult the Data Security Group if needed.
- Do not save copies of personal data to personal computers. Access and update the central copy.

4.2. Data Processing

4.2.1. Fair and Lawful Processing:

4.2.1.1. Ensure all processing is lawful, fair, and transparent.

4.2.1.2. Inform individuals about:

- The identity and contact details of the data controller (Apogee).
- The contact details of the Data Protection Officer (if applicable).

- The purposes of the processing.
- The recipients or categories of recipients of the personal data.

4.2.1.3. Obtain explicit consent for processing special categories of personal data (sensitive data) unless an exception applies.

4.2.1.4. When processing special categories of personal data, Apogee will ensure that one of the following additional conditions is met:

- Explicit consent from the data subject
- Processing is necessary for employment, social security, or social protection purposes
- Processing relates to data manifestly made public by the data subject
- Processing is necessary for legal claims or judicial acts
- Processing is necessary for substantial public interest reasons
- Processing is necessary for preventive or occupational medicine, medical diagnosis, or healthcare provision
- Processing is necessary for public health purposes
- Processing is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes

4.2.1.5. Apogee relies on the following lawful bases for processing personal data:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

4.2.1.6. The appropriate lawful basis will be determined and documented for each processing activity.

4.2.2. Processing for Limited Purposes:

4.2.2.1. Process personal data only for the specific purposes for which it was collected.

4.2.2.2. If the purpose changes, inform the individuals and obtain new consent if necessary.

4.2.3. Adequate, Relevant and Non-Excessive Processing:

4.2.3.1. Collect and process only the personal data necessary for the specific purpose

4.2.4. Accurate Data:

4.2.4.1. Maintain accurate and up to date personal data.

4.2.4.2. Take steps to ensure accuracy at collection and at regular intervals

4.2.4.3. Destroy inaccurate or outdated data.

4.2.5. Timely Processing:

4.2.5.1. Do not keep personal data longer than necessary for the purpose it was collected.

4.2.5.2. Follow the Apogee Data Retention Policy for guidance.

4.2.6. Processing in Line with Data Subjects rights:

4.2.6.1. Respect and facilitate the exercise of data subject rights, including the right to:

- Access
- Rectification
- Erasure
- Restriction of processing
- Data portability
- Object
- Not be subject to automated decision-making including profiling

4.2.6.2. Apogee will respond to subject access requests within one month of receipt.

4.2.6.3. If Apogee engages in automated decision-making or profiling that has a legal or significant effect on individuals, it will implement appropriate safeguards and provide individuals with information about the logic involved, as well as the significance and envisaged consequences of such processing.

5. Consequences

5.1. Business Consequences

5.1.1. **Regulatory Sanctions**: Non-compliance with data protection laws can result in significant fines and penalties from regulatory authorities. This includes not only the Information Commissioner's Office (ICO) in the **UK**, but also the following data protection authorities in other jurisdictions where Apogee operates:

5.1.1.1. **Germany**: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

5.1.1.2. **France:** Commission Nationale de l'Informatique et des Libertés (CNIL)

5.1.1.3. **Jersey:** Office of the Information Commissioner (OIC)

5.1.1.4. **Isle of Man:** Information Commissioner * Ireland: Data Protection Commission (DPC)

5.1.2. **Reputational Damage**: Data breaches and privacy violations can severely damage Apogee's reputation, leading to loss of customer trust and business opportunities.

5.1.3. **Legal Action**: Apogee may face legal action from individuals whose data has been mishandled, resulting in financial losses and further reputational harm.

5.1.4. **Operational Disruption:** Data breaches and security incidents can disrupt business operations, leading to downtime, productivity losses, and increased costs.

5.2. Individual Consequences

5.2.1. **Disciplinary Action**: Employees who violate this Data Protection Policy may face disciplinary action, up to and including termination of employment. This may include:

- Verbal or written warnings.
- Suspension.
- Demotion.
- Dismissal.

5.2.2. **Personal Liability:** In certain circumstances, individuals may be held personally liable for data protection breaches, leading to potential fines and legal action.

5.2.3. **Whistleblower Protection:** Employees are encouraged to report any data protection concerns without fear of retaliation. Apogee will protect individuals who report concerns in good faith.

5.3. Reporting and Investigation

5.3.1. **Reporting:** Any suspected or actual data protection breaches or security incidents must be reported immediately to the Data Security Group or the Compliance Department.

5.3.2. **Investigation**: All reported incidents will be promptly investigated to determine the cause, extent, and impact of the breach.

5.3.3. **Remedial Action:** Appropriate remedial action will be taken to address the breach, prevent future incidents, and mitigate any harm to individuals.

5.4. Additional Considerations

5.4.1. **Severity:** The consequences of non-compliance will vary depending on the severity of the breach and the level of harm caused to individuals.

5.4.2. **Intentional vs. Unintentional:** Intentional breaches or negligence may result in more severe consequences than unintentional errors.

Apogee takes data protection seriously and expects all employees to adhere to this policy. By understanding and following these guidelines, employees can help protect the personal data entrusted to Apogee and avoid the negative consequences of non-compliance.

6. Reporting and Policy Review

6.1. Monitoring and Reporting

Apogee is committed to maintaining a robust monitoring and reporting framework to proactively identify and address any potential risks to data protection compliance and good customer outcomes. This framework will include:

- **Regular Audits and Assessments**: Conduct periodic internal audits and assessments to evaluate the effectiveness of data protection controls and identify areas for improvement.
- **Data Breach Reporting**: Implement clear procedures for reporting and investigating data breaches, including timely notification to affected individuals and relevant regulatory authorities when required.
- **Key Performance Indicators (KPIs):** Establish and track KPIs to measure the effectiveness of the data protection program, such as the number of data breaches, subject access requests, and employee training completion rates.
- **Management Reporting**: Provide regular reports to senior management and the Audit and Risk Committee on data protection compliance, risks, and incidents.

6.2. Policy Review

This Data Protection Policy will be reviewed at least annually or more frequently, if necessary, to ensure it remains aligned with evolving data protection laws, regulations, and best practices. The review will assess the policy's effectiveness in achieving good customer outcomes and identify any areas for improvement.

The review process will involve:

- **Consultation:** Consult with relevant stakeholders, including the Data Security Group, Compliance Department, Legal Department, and representatives from business units that handle personal data.
- **Legal and Regulatory Updates:** Assess any changes in data protection laws and regulations and incorporate them into the policy as needed.
- **Technological Advancements:** Evaluate the impact of new technologies on data processing activities and update the policy to address any emerging risks.
- **Policy Approval:** Submit any proposed changes to the policy to the Albacore (Apogee) Board for approval.

Document Control

DOCUMENT NAME	VERSION	MASTER COPY LOCATION
Data Protection 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 document
2	2024/09/23	Keith Harvey	• Restructured the policy for improved clarity and organisation. • Revised and expanded the "Roles and Responsibilities" section to clarify accountabilities and include the Data Protection Officer. • Enhanced the "Policy Requirements" section with more specific guidance on data handling, security, and processing, aligning with best practices.

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	2024-09-24	Robert Marr	DPO/Head of Legal
2	2024-09-24	Simon Green	Chief Information Officer
2	2024-09-24	Samantha Jackson	Chief Finance Officer
2	2024-09-24	Marion Brooks	Chief People Officer
2	2024-09-24	James Clark	Chief Executive Officer

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	Approved
2	2024-09-24	James Clark	Chief Executive Officer	Approved