



Data Governance & GDPR POLICY

Applicable to Curlew Capital Ltd, its subsidiaries, and all funds under its management (collectively, "Curlew").

Effective Date: January 2026

Approved by: Chief Executive Officer and Board of Directors

1. Introduction

Curlew Capital Ltd. ("the Company" or "Curlew") recognizes the importance of managing and governing data to maintain its integrity, availability, and confidentiality. The Data Governance Policy outlines the framework, principles, roles, and responsibilities necessary for managing data across the organization in a manner that supports the Company's strategic goals and complies with applicable regulations, including the General Data Protection Regulation (GDPR).

This policy applies to all employees, contractors, and third parties who process personal data on behalf of the Company.

Personal data includes any information relating to an identified or identifiable individual.

2. Purpose

The purpose of this policy is to ensure:

- The Company's data is of high quality, accurate, secure, and used responsibly.
- Compliance with legal, regulatory, and business requirements.
- Roles and responsibilities for data governance are clearly defined and understood across the organization.

3. Scope

This policy applies to all data owned, processed, and managed by Curlew Capital Ltd., including:

- Client data: Identification details, financial information, communications, and portfolio data.
- Employee data: HR records, payroll information, and performance evaluations.
- Financial data: Company accounts, transactions, and tax records.
- Vendor and partner data: Contracts, terms, and communications.



It applies to all employees, contractors, and third-party service providers who interact with or manage the Company's data.

4. Data Governance Principles

Curlew Capital Ltd. adopts the following key principles to guide its data governance practices:

- **Accountability:** All data owners are responsible for ensuring the proper management and protection of data under their control.
- **Integrity:** Data should be accurate, reliable, and trusted.
- **Protection:** All data must be adequately protected from unauthorized access, loss, or corruption through appropriate technical and organizational measures.
- **Compliance:** Data governance practices must align with relevant laws and regulations, including GDPR and industry-specific requirements.
- **Transparency:** The use of data must be transparent, and data subjects must be informed about how their personal data is collected, stored, processed, and shared.
- **Data Minimization:** Data collected and retained should be limited to what is necessary for the purposes it is used for.
- **Availability:** Data must be available to authorized users when needed for legitimate business purposes.
- **Lifecycle Management:** Data must be managed throughout its lifecycle, from collection to deletion or archiving, in accordance with the Data Retention Policy.

5. Roles and Responsibilities

Data Protection Officer (DPO)

The DPO is responsible for:

- Overseeing data protection strategies and compliance with GDPR.
- Acting as the primary point of contact for regulatory authorities and data subjects regarding data protection matters.
- Responding to data breaches.

Data Users

All employees and contractors who handle data are responsible for:

- Complying with the Data Governance Policy and other related policies.
- Ensuring data is used only for legitimate business purposes.
- Reporting any data security incidents, breaches, or misuse to the DPO.



Further information on employee usage of and behaviour using Curlew systems can be found in the Curlew "IT and Communications Policy".

Line Managers

Line Managers are expected to ensure the following principles:

- Subordinate employee access to systems is configured to the minimum required permissions the employee requires.
- New employees will be provided with access to cyber security training via our HR platform Employment Hero within their probation period. will complete cyber security training within 3 months of employment.
- When employees leave, Line Managers must ensure that:
 - Access to Curlew systems is revoked on the last day of employment.
 - Employee user account and email address is delisted from Curlew systems.
 - Company hardware is returned.
 - Returned hardware is decommissioned appropriately, with data wiped from the item before it is recommissioned or disposed of.

Third Party IT Providers

Curlew outsources its IT infrastructure and support to third-party service providers. These third-party IT providers are responsible for:

- Implementing and maintaining data security controls: This includes ensuring appropriate encryption, access control, and secure backup processes are in place.
- Ensuring the availability and integrity of IT systems: The IT providers are responsible for maintaining uptime, performance, and the integrity of Curlew's data and systems.
- Regular monitoring and patching: Ensuring that software and systems are kept up-to-date with the latest security patches and updates to protect against vulnerabilities.
- Incident Response: Assisting in investigating and resolving IT-related incidents, such as system outages or data breaches.

Curlew Capital Ltd. maintains appropriate service level agreements (SLAs) with its IT providers to ensure these responsibilities are upheld. Currently Curlew's SLA with PSTG also provides access to a Service Desk that provides support and assistance in the use of IT equipment, including:

- Management of the prompt resolution of Incidents arising within the IT Equipment which are raised by Curlew.
- Management of the prompt resolution of Incidents arising within the IT Equipment which are identified by PSTG's monitoring system.



- Escalation management if required in the event of protracted Incident resolution.
- Management of change requests.
- Remote access support if possible and appropriate.

The Service Desk response and resolution targets are:

Priority Level	Description	Reporting Method	Response Time	Resolution Time
1	Business-critical system failure	Telephone	Immediate	Two Working Hours
2	VIP or service affecting with more than one End User affected	Telephone	Immediate	Four Working Hours
3	Single End User affected	Telephone or email	Eight Working Hours	One Working Day
4	Non-urgent, peripheral not working	Telephone or email	Eight Working Hours	One Working Day
5	Service Request for configuration change that does not require change management	Telephone or email	Eight Working Hours	Five Working Days

Note: Curllew pays for 5 "VIP" users, for whom Service Desk Cover will be extended to 24 x 7 x 365.

6. Data Security and Privacy

Curllew Capital Ltd. implements the following data security measures to protect its data:

- Access Control: Data access is restricted based on the principle of least privilege (See glossary). Only authorized personnel will have access to sensitive data.
- Encryption: Sensitive data is encrypted both at rest and in transit, in accordance with industry best practices.
- Third-Party Security: When data is shared with third parties (e.g., vendors, service providers), Curllew Capital Ltd. ensures that adequate data protection agreements are in place.
- Training: All staff are provided with access to Data Protection training undergo yearly Data Protection Training[FB3.1], provided by third party partners.

7. Data Quality and Standards

Curllew Capital Ltd. maintains an up-to-date, documented data protection policy that is communicated to all employees and relevant third parties. This policy is regularly



reviewed and updated to align with the evolving risk landscape and business operations.

8. Anti-Virus and Malware Protection

Curlew Capital Ltd. relies on third-party IT service providers to ensure that all systems are protected with up-to-date anti-virus and anti-malware software. Currently Curlew maintains an SLA with PSTG to provide protection across Curlew's IT estate including:

- Providing a fully managed and monitored endpoint security, detection and response solution with 24/7 support wraparound on Microsoft 365 Premium using Defender for Endpoint P2.
- Installation and management of security software on all systems, ensuring that anti-virus and anti-malware solutions are current and effective.
- Regular monitoring and updates to ensure the latest security patches and virus definitions are applied to all systems.
- Proactive scanning and detection of malware, viruses, and other security threats across all devices and infrastructure.
- Providing reports to continually evaluate the Curlew's security across all managed devices.
- Incident response and resolution, working with Curlew Capital Ltd. to mitigate and resolve any detected threats or vulnerabilities.

9. Cloud-Based Systems and Backup Management

Curlew Capital Ltd. uses cloud-based systems with managed backup processes. The cloud infrastructure is operated by third party providers who ensure compliance with security standards, and provide regular backups to ensure that data is protected against loss or corruption. Currently Curlew maintains an SLA with PSTG who have partnered with CyberGuard to offer a range of cloud based security solutions including:[FB4.1]

- Providing a fully managed and monitored cloud security solution with 24/7 support wraparound on Microsoft 365 Premium using Defender for Cloud Apps.
- Regular backups: Ensuring that data is backed up regularly according to agreed-upon schedules.
- Conditional Access App Control, helping to restrict the flow of data (via web access routes) from unmanaged devices.
- Threat hunting: proactively learning from current global and organisational threat landscapes to review new threats, vulnerability or exploit/malware campaigns, and turn hunting rules into new detection techniques to constantly move forward with security protocols.[FB5.1]



- Recovery testing: Periodically testing the data recovery process to ensure that data can be restored quickly and efficiently in case of accidental loss, corruption, or disaster.
- Incident response: In the event of data loss or corruption, the third-party IT providers will work to restore data promptly, minimizing disruption to business operations, the response and resolution times they are committed to are detailed below:

Priority	Time to first response	Time to resolution[FB6.1]
Critical	15 minutes	1 hour
High	30 minutes	2 hours
Medium	1 hour	4 hours
Low	4 hours	24 hours

Curlew Capital Ltd. maintains service level agreements (SLAs) with its IT providers to ensure these responsibilities are upheld, and that data can be recovered quickly and effectively.

PSTG's Backup and Recovery Service for Microsoft 365 protects Curlew against loss of data that is held within Microsoft's cloud infrastructure. PSTG will back-up Curlew's Microsoft 365 data based on the number of End Users and storage capacity set out in the SLA; backup data is stored on a backup appliance which is located at PSTG's Data Centre.[FB7.1]

Microsoft 365 backups by PSTG include:

- OneDrive file and folder data backups (documents), per End User.
- Exchange data, including emails, email attachments, notes, deleted items, contacts (excluding photographs), tasks and calendar events (including attendees, recurrence, attachments and notes).
- SharePoint primary, custom, group and team site collections; folders, document libraries and sets; site assets, templates and pages.
- Groups (including conversations, plans, files, sites and calendar).
- Teams (including wiki and chat).
- Audit logs, data controls and export capabilities.

Backups are encrypted while at rest and in transmission, and are retained for 90 days. Data restoration will only be initiated at the request of an authorized Curlew representative. PSTG will perform quarterly test restores to ensure that backups are functioning correctly.

10. Data Lifecycle Management



Data will be managed throughout its lifecycle in accordance with the following stages:

- **Data Collection:** Data is collected for legitimate purposes, and individuals are informed of how their data will be used.[FB8.1]
- **Data Use:** Data is used only for the purposes for which it was collected and in compliance with relevant laws and regulations.
- **Data Retention:** Data is retained only for as long as necessary to fulfil its purpose or comply with legal or regulatory requirements, as per the Data Retention Policy.
- **Data Disposal:** When no longer needed, data is securely deleted or anonymized to ensure it cannot be recovered or misused.

11. Compliance and Auditing

Curlew Capital Ltd. is committed to regular compliance audits to ensure adherence to this Data Governance Policy and other related policies. Internal and external audits are conducted to review data management practices, identify areas for improvement, and ensure compliance with relevant regulations such as GDPR[FB9.1].

12. Policy Review

This Data Governance Policy will be reviewed annually, or whenever significant changes in business operations, technology, or regulatory requirements occur. Any changes to the policy will be communicated to all relevant staff and stakeholders.

13. Approval

Approved by: Charlie Oliver
Chief Executive Officer
Curlew Capital Ltd

Version: 2026