Data Protection Policy

Classification: Public

Data Protection Policy Statement

New Era Technology and its subsidiaries (collectively the “Company” or “New Era”) are committed to implementing the necessary requirements to protect the confidentiality, integrity, and availability of all personal and organisational data entrusted to us. We uphold the highest standards of data protection and privacy across all jurisdictions where we operate, ensuring compliance with applicable laws and regulations worldwide.

This Policy applies to all individuals who create, access, process, or manage personal or organisational data within New Era Technology, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All users are expected to act responsibly and in accordance with established procedures to safeguard data and uphold privacy obligations.

New Era will implement and maintain controls to ensure that:

- Lawful and Transparent Processing: Personal data is processed fairly, lawfully, and for legitimate purposes.
- Privacy and Security by Design: Privacy and security principles are embedded into systems, processes, and services.
- Data Subject Rights: Individuals’ rights to access, correct, erase, restrict, and transfer their data are respected and facilitated.
- Global Compliance: All activities comply with applicable data protection and privacy laws, including those governing sensitive health and financial information.
- Continuous Improvement: Controls are regularly reviewed and enhanced to address evolving risks and regulatory requirements.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
'Data Protection Law'	includes the UK and EU GDPR, US HIPAA/HITECH and relevant state laws, e.g., CA CCPA/CPRA, Canada PIPEDA, Brazil LGPD, Australia Privacy Act, China PIPL, and any other international data protection laws/rules/regulations applicable to New Era or to those entities processing personal data on New Era's behalf.
"staff", "users", "personnel"	means those who are employed by New Era Technology on a fulltime, part-time, or temporary basis; those who access and / or utilize New Era Technology's information resources, including, but not limited to employees, contractors, interns, third and external parties.
"we", "our", "New Era", or "New Era Technology"	refers to New Era Technology and its subsidiaries.

2. Scope

This Policy applies to all New Era Technology's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

The terms set out in this Policy work in conjunction with, and do not replace, amend, or supplement any terms or conditions of employment stated in any collective bargaining agreements and/or employment contracts.

In regions where specific Data Protection Law applies, New Era will comply with such laws, rules, and regulations alongside this policy. For clarity, this policy is not intended to restrict communications or actions protected or required by regional/local laws and regulations.

Relationship with Local/Regional Policies

This Data Protection Policy is New Era's corporate policy. New Era Technology business units and/or subsidiaries may complement this with a local/regional data protection however, this Policy shall always be the minimum standard; a local/regional policy may augment, or increase the standards, but shall not detract from the New Era Technology data protection standards.

If any additional data protection policies are developed, Director of Governance, Risk and Compliance (GRC) must review and approve prior to release and publication.

3. Roles and Responsibilities

The Director of Governance, Risk and Compliance (GRC), Chief Information Officer (CIO) and the Chief Technology Officer (CTO) are responsible for the New Era Technology Security framework and its associated policies.

This Policy is reviewed annually by members of GRC. Any changes to this Policy will be approved by New Era Technology's CIO, CTO and Director of Governance, Risk, and Compliance prior to its release.

Suggestions for change to this Policy should be reported to GRC@neweratech.com.

All employees, contractors, vendors, service providers, and/or any other third parties processing personal data on New Era's behalf shall comply with applicable Data Protection Law in their respective jurisdictions.

Technology owners are responsible for technical standards applicable to their operating environments and domains.

Line managers have day–to–day responsibility for this policy, and employees should refer any questions about this policy to them in the first instance.

In line with their applicable solutions groups, New Era's business units shall develop, disseminate, and maintain formal, documented processes and/or procedures to facilitate the implementation of this Policy and, where applicable, any local/regional security or information security policies.

The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

New Era Technology is committed to processing personal data, including special category and sensitive data, in compliance with applicable Data Protection Laws globally. This includes, but is not limited to, GDPR (UK & EU), HIPAA (US), PIPEDA (Canada), and other relevant regional regulations.

We process personal data of individuals worldwide, including employees, clients, partners, suppliers, and other third parties. Our approach ensures:

- Legal Basis for Processing: All processing activities are based on lawful grounds such as consent, contractual necessity, legal obligation, legitimate interests, vital interests, or public interest.
- Privacy Notices: Clear, accessible notices explain how and why data is processed and outline individuals' rights.
- Data Minimisation and Purpose Limitation: We collect only what is necessary and use it solely for defined purposes.
- Retention and Disposal: Data is retained only as long as necessary and securely erased or anonymised thereafter.
- Security Measures: Technical and organisational controls protect data against unauthorised access, loss, or misuse.
- Cross-Border Transfers: Transfers outside local jurisdictions are safeguarded through appropriate mechanisms (e.g., contractual clauses, adequacy decisions).
- Privacy by Design and Default: We embed privacy principles into systems and processes from the outset.
- Incident Response: We maintain procedures for detecting, reporting, and responding to personal data breaches promptly.

Data Protection Principles

New Era complies with the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

Process / Procedures / Guidance

New Era will:

- Identify lawful basis for processing in advance and ensure compliance with applicable Data Protection Law. This may include:
    - Consent (clear, informed)
    - Contractual necessity
    - Legal obligation
    - Legitimate interests (balanced against rights)
    - Vital interests
    - Public interest or official authority
- Not process personal data in ways that are inconsistent with the purposes described in this Policy or the applicable privacy notice.
- Ensure privacy notices are in place advising employees, client and others of the legal basis for processing their data, how and why their data is being processed, and, their rights.
- Collect and process only necessary data for identified purposes.
- Ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible.
- Maintain accuracy and systems to keep data up to date.
- Only hold onto personal data for as long as it is needed for the purposes for which it was collected,
- Apply retention schedules and securely erase or anonymise data when no longer needed.
- Implement security measures (encryption, access control, monitoring, secure disposal).
- Manage cross-border transfers with documented safeguards.
- Train and supervise staff who handle personal data; maintain awareness programmes.
- Operate an incident response process for prompt detection, reporting, containment, and notification of breaches.
- Facilitate data subject rights requests without undue delay and within statutory timelines.
- Conduct Data Processing Impact Assessments (DPIAs) for high-risk processing and maintain Records of Processing Activities (ROPA).
- Audit and review compliance regularly.

Data Subject Rights

We enable and respond to the following rights without undue delay and within statutory timelines:

- Access: Confirmation of processing, copy of data, and related information.
- Rectification: Correct inaccurate or incomplete data.

- Erasure: Delete data where no longer necessary, consent withdrawn, or legally required.
- Restriction: Limit processing under defined conditions.
- Portability: Provide a copy of data in a portable format where applicable.
- Objection: Object to processing based on legitimate interests or for direct marketing.
- Automated Decision-Making: Safeguards and rights related to profiling.

Special Category Personal Data (often referred to as Sensitive Personal Data)

This includes the following personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data or biometric data
- Health data
- Sex life or sexual orientation
- Criminal convictions or offences

Processing occurs only where:

- Explicit consent has been given.
- Necessary for employment law obligations.
- Vital interests apply.
- Data is manifestly public.
- Required for legal claims.
- Substantial public interest applies.

5. Compliance, Monitoring and Enforcement

This Policy is intended for all New Era businesses, in all countries.

New Era Technology seeks to proactively prevent and mitigate instances of non–compliance with this Policy.

Compliance is measured through various methods, including but not limited to risk assessments, business tool reports, internal and external audits, etc.

Any breaches or concerns, including ethical concerns or potential breaches in our commitment to information and data protection standards, should be reported as soon as possible through our Whistleblowing Policy.

Any need for improvements will be applied as soon as possible. Employees are encouraged to offer their feedback on this Policy if they have any suggestions for how it may be improved. Feedback of this nature should be addressed to GRC@neweratech.com.

Any exception to this Policy must be approved by the CTO, CIO, and / or Director of Governance, Risk, and Compliance in advance.

Personnel found to have intentionally violated this Policy may be subject to disciplinary action, up to and including termination of employment and other penalties as set forth herein. New Era Technology reserves the right to pursue any, and all, legal and civil action in connection with any such violation.

Any vendor, consultant, or contractor found to have violated this Policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

6. Acknowledgement

Those in receipt of this Policy acknowledge its receipt and understanding of its contents; and that New Era Technology expressly reserves the right to change, modify, or delete its provisions without notice.

Document Information

Reference	Privacy Framework
Title	Data Protection Policy
Purpose	The purpose of this policy is to provide information about data protection principles that we, New Era, must comply.
Owner	Governance, Risk & Compliance (GRC)
Document Approvers	Chief Information Officer (CIO) Chief Technology Officer (CTO) Director of Governance, Risk & Compliance (GRC)
Intended Audience	New Era Technology management, personnel and interested parties.
Review Plan	Annually
Document Classification	Public

Document History

VERSION CONTROL			
Revision	**Date**	**Record of Changes**	**Approved /Released By**
V1.0	May 2022	Approved release	GRCI Law, Dir GRC
V2.0	Jun 2024	Reviewed	Dir GRC
V3.0	Sep 2024	Annual review, updates to sections 2-6	Legal, Dir GRC
V3.0	Oct 2024	Approved release	CTO, Dir GRC
V4.0	Jan 2026	Annual review, updates, approval	CTO, CIO, Dir GRC

References

Standard / Framework / Other	Title	Description
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements	Requirements for establishing, implementing, maintaining, and continually improving an ISMS.
ISO/IEC 27002:2022	Code of Practice for Information Security Controls	Guidance on implementing information security controls.
ISO/IEC 27701:2019	Privacy Information Management System (PIMS)	Extension to ISO 27001 for managing privacy and personal data protection.
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations	Catalog of security and privacy controls for information systems and organizations.
GDPR (UK & EU)	General Data Protection Regulation	Legal framework for data protection and privacy in the UK and EU.
HIPAA (US)	Health Insurance Portability and Accountability Act	US regulation for safeguarding protected health information (PHI).
PIPEDA (Canada)	Personal Information Protection and Electronic Documents Act	Canadian law governing personal data in commercial activities.