

SECTION 01 | POLICY FOUNDATION

OUR COMMITMENT

At Senan Holding, we protect the privacy, confidentiality and security of personal data entrusted to us. Across our people, projects, businesses and digital channels, we use information responsibly, for clear business purposes, and with safeguards proportionate to the sensitivity of the information and the associated risk.

PURPOSE & SCOPE

This Policy explains how Senan Holding and relevant Group entities collect, use, share, retain and protect personal data. It applies to directors, officers, employees, applicants, clients, visitors, suppliers, subcontractors, consultants and other parties who provide, access or process personal data in connection with Senan Holding.

KEY DEFINITIONS

- Personal data is any information that identifies, or can reasonably be linked to, an individual. Processing includes collecting, recording, organizing, storing, using, sharing, transferring, restricting, deleting or destroying that information.
- Data subject means the individual to whom personal data relates. The relevant Senan Holding entity may act as the data controller where it determines the purpose and means of processing.
- Sensitive or restricted data includes information such as government identifiers, health or biometric data, financial details, legal records and other information subject to enhanced protection.

POLICY PRINCIPLES

- Process personal data lawfully, fairly and transparently for legitimate, defined business purposes.
- Collect only what is relevant and necessary, keep it accurate, and retain it only for an appropriate period.
- Respect confidentiality and individual rights, while applying security measures appropriate to the information and risk.
- Limit access and sharing to authorized persons and approved purposes.

ACCOUNTABILITY & COMPLIANCE

- Every person covered by this Policy is responsible for following it. Managers must lead by example, support training and address non-compliance promptly.
- Suspected misuse, unauthorized access, loss or disclosure of personal data must be reported without delay through the appropriate internal channel.
- Deliberate or serious breaches may lead to disciplinary action, up to and including termination of employment or engagement, subject to applicable rules and due process.

POLICY STATUS & REVIEW

This Policy is a statement of Senan Holding standards and does not replace applicable law, contractual commitments or detailed procedures. It will be reviewed periodically and may be updated to reflect changes in the Group, technology, risk or legal requirements.

DATA PROTECTION & INFORMATION SECURITY

PRIVACY | SECURITY | ACCOUNTABILITY

SECTION 02 | COLLECTION & USE OF PERSONAL DATA

RESPONSIBLE COLLECTION & USE

We collect and process personal data only where it is necessary to operate safely and efficiently, manage our workforce and projects, deliver services, meet contractual or legal obligations, protect people and property, and maintain trusted business relationships.

LAWFUL & PURPOSEFUL PROCESSING

- Where required, processing is based on an appropriate legal ground, such as consent, contractual necessity, legal obligation, legitimate interests, vital interests or legal claims.
- Sensitive or restricted data is processed only when genuinely necessary and permitted by applicable requirements, with additional safeguards where appropriate.
- We do not use personal data for a purpose that is incompatible with the reason it was collected, unless permitted or required by law.

TYPES OF DATA WE MAY PROCESS

- Identity and contact data: name, address, telephone, email, emergency contact and identification details.
- Employment and professional data: applications, qualifications, references, payroll, benefits, training, performance and work records.
- Security and operational data: visitor or site-access records, access credentials, CCTV or incident records where used and permitted.
- Digital and technical data: device, account, system-log, IP-address and communication data generated through approved systems.

HOW DATA IS OBTAINED & USED

- We may receive data directly from individuals through application forms, contracts, onboarding records, correspondence, site access procedures, surveys, support requests and other business interactions.
- Data may be generated during the relationship with Senan Holding, including payroll, timekeeping, project allocation, training, performance, benefits, travel, health-and-safety or disciplinary records where relevant and lawful.
- We may obtain limited data from legitimate third-party sources, such as recruitment platforms, professional referees, service providers, insurers, medical or occupational providers, educational institutions, authorities and business partners, where permitted.
- Typical purposes include recruitment; employment administration; access control and workplace security; payroll and benefits; project and contract delivery; supplier due diligence; emergency response; compliance; internal investigations; and responding to enquiries.

DATA QUALITY & MINIMISATION

Individuals should keep their information accurate and notify the Group of material changes. Senan Holding will take reasonable steps to verify, correct and update data where appropriate, and to reduce collection or use that is unnecessary for the stated purpose.

SECTION 03 | DIGITAL PRIVACY & DATA SHARING

TRANSPARENCY & TRUSTED SHARING

We communicate clearly about our data practices, maintain information accurately, and limit disclosure to legitimate and controlled business needs. Personal data is not shared simply because it is available; it is shared only where there is a valid purpose, authority and appropriate protection.

WEBSITE, COOKIES & ONLINE ENQUIRIES

- When someone contacts Senan Holding through our website, social-media channels or email, we use the information to respond, provide requested material and improve the quality of our communications and services.
- Our digital channels may use essential cookies and, where applicable, analytics technologies. When non-essential tools are used, the relevant notice and choice mechanism will be provided.
- Online analytics are used in a manner that supports website performance, security and user experience, subject to applicable requirements.

EXTERNAL LINKS & INDEPENDENT SITES

- Our websites may link to third-party websites for convenience or information. Those sites are operated independently and have their own privacy practices.
- Senan Holding is not responsible for the content, security or privacy approach of an external website. Users should review the privacy notice of any third party before submitting personal data.
- We do not provide personal data to an external site merely by placing a link to it.

SHARING & DISCLOSURE

- Personal data may be shared with approved Group companies, clients, service providers, subcontractors, professional advisers, insurers, banks, auditors, technology providers or other recipients who need it to perform an authorized service or transaction.
- We may disclose information to authorities, courts, regulators or emergency services where required or permitted by law, or where necessary to protect legal rights, safety or security.
- Recipients must use information only for the approved purpose and must apply appropriate confidentiality, security and contractual controls.

THIRD PARTIES, TRANSFERS & CHILDREN

- Third parties that process personal data for Senan Holding are assessed as appropriate and must meet relevant privacy and information-security requirements.
- Where data is transferred across borders or hosted outside the country in which it was collected, Senan Holding will use appropriate safeguards and comply with applicable transfer requirements.
- We do not intentionally collect personal data from children directly unless this is necessary, lawful and supported by the appropriate parent, guardian or other legal authorization.

NO UNAUTHORISED SECONDARY USE

Senan Holding does not permit personal data to be used by a recipient for unrelated purposes. We do not sell personal data as a commercial product, and we do not disclose it without a lawful or authorized basis.

DATA PROTECTION & INFORMATION SECURITY

PRIVACY | SECURITY | ACCOUNTABILITY

SECTION 04 | INFORMATION SECURITY & RETENTION

INFORMATION SECURITY IS EVERYONE'S RESPONSIBILITY

Personal data must be protected whether it is held on paper, in a system, on a mobile device, in an email, in an image or discussed verbally. Senan Holding uses organizational, technical and physical safeguards to reduce the risk of loss, misuse, unauthorized access, alteration or disclosure.

SECURITY CONTROLS

- Security controls may include role-based access, secure account management, strong passwords and authentication, encryption or equivalent protection, secure servers and networks, firewalls, backups, antivirus or endpoint protection, and monitored access to sensitive systems.
- Access is granted on a need-to-know basis, reviewed as roles change, and removed promptly when no longer required. Information must be kept in approved systems, storage locations and repositories.
- Physical controls, such as secured rooms, locked cabinets, controlled site access and clear-desk practices, support the protection of paper files and devices.

SECURE WORKING PRACTICES

- Lock screens or secure devices when unattended, and prevent personal data from being visible to unauthorized persons.
- Use only approved devices, accounts, cloud services, applications and file-sharing methods. Do not store Company data on personal drives, personal email or unapproved messaging platforms.
- Verify the identity and authority of a caller or requester before discussing or releasing personal data. Escalate suspicious or pressurized requests.
- Keep portable media and printed information secure, encrypt or password-protect where appropriate, and report a lost device or misdirected message immediately.

SUPPLIERS, CLOUD & REMOTE WORKING

- Any supplier or cloud service that processes personal data for Senan Holding must be approved through the appropriate business, procurement, privacy and security process.
- Contracts should include suitable confidentiality, data-protection and security obligations, together with requirements to report incidents and support investigations.
- Remote and site-based work must follow the same protection standards. Personnel must take reasonable steps to secure paper files, devices, networks and conversations outside normal office locations.

RETENTION, ARCHIVING & SECURE DISPOSAL

Personal data is retained in accordance with a documented retention schedule, taking account of its purpose, contractual needs, legal or regulatory duties, tax or accounting requirements, health-and-safety obligations and the period needed to establish, exercise or defend legal claims. When information is no longer required, it is deleted, anonymised or securely destroyed. Paper records are shredded or otherwise made unreadable, and electronic media is disposed of or sanitized using approved methods.

SECTION 05 | RIGHTS, INCIDENTS & GOVERNANCE

RIGHTS, REPORTING & CONTINUOUS IMPROVEMENT

Senan Holding supports the rights of individuals, treats privacy concerns seriously and responds to incidents with urgency and care. We maintain governance, training and review processes to improve our safeguards as the business, risks and legal environment evolve.

INDIVIDUAL RIGHTS & REQUESTS

- Subject to applicable law, individuals may have rights to be informed, access their data, correct inaccurate information, withdraw consent, object to certain processing, request restriction or deletion, receive portable data, seek compensation or make a complaint.
- Requests will be handled through the appropriate privacy contact and may require reasonable verification of identity. Some rights may be limited where a lawful exemption applies.

PRIVACY IMPACT ASSESSMENTS

- Before introducing or materially changing a process that may create elevated privacy risk, Senan Holding may assess the necessity, proportionality and potential impact on individuals.
- The assessment considers the purpose of the processing, the data involved, potential risks, safeguards, alternatives and any actions needed to reduce risk before implementation.

INCIDENT & BREACH RESPONSE

- Any suspected loss, unauthorized access, phishing event, mistaken disclosure, device loss, data corruption or other privacy or security incident must be reported promptly.
- Senan Holding will investigate, record and manage incidents, contain harm, preserve evidence, take corrective action and notify relevant authorities or affected individuals when required by applicable law.
- Personnel must cooperate fully with authorized investigations, audits and legal or regulatory reviews.

RESPONSIBILITIES & TRAINING

- Personnel with access to personal data must use it only for authorized purposes, keep it confidential and protect it in line with this Policy and related procedures.
- All relevant personnel receive privacy and security awareness as part of onboarding and at suitable intervals thereafter. Enhanced instruction is provided where roles involve regular access to sensitive data or higher-risk processing.
- Managers are responsible for maintaining a culture in which questions and concerns are raised early and handled fairly.

GOVERNANCE, CONTACT & REVIEW

Group Management is responsible for oversight of this Policy, supported by designated privacy, legal, HR, IT and security stakeholders as appropriate. For a privacy question, request, feedback or complaint, please use the official Senan Holding contact channels published on this website and mark your communication for the attention of the Privacy Office. This Policy is reviewed at least annually and updated when necessary to reflect changes in law, business operations, technology or risk.