Knoco Limited

Privacy Policy Notice and other Policies

Contents:

This policies document will be adhered to by all Directors and staff of the Knoco Ltd, partnership companies and sub contractors, when providing services or conducting business under the Knoco brand.

Privacy Policy Notice

This privacy policy notice is for this website; www.knoco.com, and served by Knoco Ltd, 37 Portland Road Kilmarnock, KA1 2DJ, and governs the privacy of those who use it. The purpose of this policy is to explain to you how we control, process, handle and protect your personal information while browsing or using this website, including your rights under current laws and regulations. If you do not agree to the following policy you may wish to cease viewing / using this website.

Policy key definitions:

- "I", "our", "us", or "we" refer to the business, [Business name & other trading names].
- "you", "the user" refer to the person(s) using this website.
- GDPR means General Data Protection Regulation
- PECR means Privacy & Electronic Communications Regulation.
- ICO means Information Commissioner's Office.
- Cookies mean small files stored on a user's computer or device.

Processing of your personal data

We are registered with the ICO under the Data Protection Register, our registration number is: ZA009465.

Internet cookies

We use cookies on this website to provide you with a better user experience. We do this by placing a small text file on your device / computer hard drive to track how you use the website, to record or log whether you have seen particular messages that we display, to keep you logged into the website where applicable, to display relevant adverts or content, referred you to a third party website.

Some cookies are required to enjoy and use the full functionality of this website.

We use a cookie control system which allows you to accept the use of cookies, and control which cookies are saved to your device / computer. Some cookies will be saved for specific time periods, where others may last indefinitely. Your web browser should provide you with the controls to manage and delete cookies from your device, please see your web browser options.

Cookies that we use are;

- Google Analytics

Data security and protection

We ensure the security of any personal information we hold by using secure data storage technologies and precise procedures in how we store, access and manage that information. Our methods meet the GDPR compliance requirement and are described in the Knoco information and data protection policy.

Information and Data Protection Policy

Our Company Data Protection Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

Who is covered under the Data Protection Policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Under the GDPR (General Data Protection Regulation) we control and / or process any personal information about you electronically using the following lawful bases.

Lawful basis: Consent
The reason we use this basis: In order to maintain communication with you at your request or with your consent, as a result of you contacting us personally, by email or by online form, or subscribing to our newsletter.
We process your information in the following ways: retaining contact details and other details you share with us, under the provisions of our information and data protection policy; retaining the evidence for your consent
Data retention period: We will continue to process your information under this basis until you withdraw consent or it is determined your consent no longer exists.
Sharing your information: We do not share your information with third parties, other than contact details you submit when requesting newsletter subscription, which are handled by our EMS provider.

Lawful basis: Contract
The reason we use this basis: to fulfil our contractual obligations to you; or because you have asked you to do something before entering into a contract (e.g. provide a quote)
We process your information in the following ways: retaining contact details and other personal details and other information and data you share with us as required by the contract, under the provisions of our information and data protection policy.
Data retention period: We shall continue to process your information until the contract between us ends or is terminated under any contract terms.
Sharing your information: We do not share your information with third parties.

Lawful basis: Legal obligation
The reason we use this basis: if we need to process the personal data to comply with a common law or statutory obligation.
We process your information in the following ways: retaining contact details and other details you share with us, under the provisions of our data protection policy
Data retention period: We shall continue to process your information until the legal obligation ends
Sharing your information: We do not share your information with third parties.

Lawful basis: Legitimate interests
The reason we use this basis: if we intend to use the data in ways you would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
We process your information in the following ways: retaining contact details and other details you share with us, under the provisions of our data protection policy
Data retention period: We shall continue to process your information until the period of legitimate interest ends
Sharing your information: We do not share your information with third parties. / We do share your personal information with third parties and they include; .

If, as determined by us, the lawful basis upon which we process your personal information changes, we will notify you about the change and any new lawful basis to be used if required. We shall stop processing your personal information if the lawful basis used is no longer relevant.

Your individual rights

Under the GDPR your rights are as follows. You can read more about your rights in details here;

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

You also have the right to complain to the ICO [www.ico.org.uk] if you feel there is a problem with the way we are handling your data.

Our company collects your information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only

- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties, specifically by
    - Ensuring all laptops are password protected;
    - All USB sticks and external hard drives containing personal data are encrypted;
    - All emails to wide distribution lists, or to addressees who do not know each other, are done through BCC,
    - Shredding all Knoco or client-related documents prior to disposal or recycling.

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected, through email signatures and website statements.
- Inform people about how we'll process their data, through email signatures and website statements.
- Inform people about who has access to their information, through email signatures and website statements.
- Have provisions in cases of lost, corrupted or compromised data, through back-up of contact files.
- Allow people to request that we modify, erase, reduce or correct data contained in our databases, through contacting their local Knoco representative.

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions appear on our website.

Knoco e-Newsletter Marketing Policy

Under the GDPR we use the consent lawful basis for anyone subscribing to our newsletter or marketing mailing list. We only collect certain data about you, as detailed below. Any email marketing messages we send are done so through an EMS, email marketing service provider. An EMS is a third party service provider of software / applications that allows marketers to send out email marketing campaigns to a list of users. Our EMS provider is Campaign Monitor. We hold the following information about you within our EMS system;

- Email address
- I.P address
- Subscription time & date
- Name and Company (if provided)

Email marketing messages that we send may contain tracking beacons / tracked clickable links or similar server technologies in order to track subscriber activity within email marketing messages. Where used, such marketing messages may record a range of data such as; times, dates, I.P addresses, opens, clicks, forwards, geographic and demographic data. Such data, within its limitations will show the activity each subscriber made for that email campaign.

Any email marketing messages we send are in accordance with the GDPR and the PECR. We provide you with an easy method to withdraw your consent (an unsubscribe link is enclosed in each newsletter) and to manage your preferences / the information we hold about you at any time. See any marketing messages for instructions on how to unsubscribe or manage your preferences, otherwise contact the EMS provider.

Information Security and confidentiality policy

Knoco will keep client material, and all Knoco material, confidential. Any exchange of confidential material with a client will be covered by a two-way confidentiality agreement, or agreements. All Knoco staff working with that client will be made aware of the agreement, and will be asked to commit to abide by it.

All Knoco laptops must have a power-on password. Screensavers must be password-protected. All external hard drives must be provided with the capability for encryption, and encrypted when not in private secure premises (hotel rooms should be treated as public). Unencrypted USB drives may be used for short term storage and transfer, but content must be deleted as soon as possible. Any additional security requirements of the client must be strictly adhered to.

Care must be taken when using third-party or cloud-based services such as Google Docs or Dropbox. These should not be used for storing confidential client data unless such data are encrypted.

All client files must be kept in secure premises, and shredded before disposal or recycling.

All client files should be backed up; ideally being stored in 3 locations, one being cloud storage.

Security Statement

Knoco has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.

This includes:

- Adopting an information and data security policy (see above)
- Taking steps to control physical security (projects and staff records are all kept in a locked filing cabinet)
- Putting in place controls on access to information (password protection on files and server access)
- Establishing a business continuity/disaster recovery plan (Knoco takes regular back-ups of its computer data files and this is stored in encrypted form in the cloud
- Detecting and investigating breaches of security should they occur

All Knoco franchisees, affiliates and subcontractors are required to comply with this security policy.

Third party social media services use servers that are outside of our control. Knoco directors, staff, franchisees and associates will keep all passwords to such services secure.

In addition, Knoco directors, staff, associates and franchisees will abide by client information security requirements and policies when working for any particular client.

Information and data breach policy

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents. The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

A data security breach, confirmed or suspected, is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage or loss to information or data held by Knoco, or an affiliate, franchisee or subcontractor, relating either to Knoco intellectual property, or to personal or client data related to a Knoco contract or Knoco marketing activity. An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- equipment or system failure, through malicious attack or hardware/software failure;
- unauthorised use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);

- unauthorised disclosure of sensitive / confidential data, either deliberate, accidental or as a result of pfishing or other online deception;
- unforeseen circumstances such as a fire or flood;
- human error.

Reporting an incident

Any individual who accesses, uses or manages the information relating to Knoco intellectual property, or to personal or client data related to a Knoco contract or Knoco marketing activity, is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO) (Nick Milton). The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved.

Containment and recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach, establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause, and plan a course of action. The police will be notified in the case of equipment theft.

Investigation and risk assessment

The DPO will conduct an investigation within 24 hours of the breach being discovered / reported. If the breach happened at the premises of a Knoco affiliate or subcontractor, the DPO will delegate the investigation to an Investigating Officer (IO). The DPO/IO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation will take into account the following:

- the type of data involved;
- its sensitivity;
- the protections that are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen;
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to the breach.

Notification

The DPO, in consultation with relevant colleagues and advisors will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible. Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation;
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.

Individuals will also be provided with a way in which they can contact Knoco for further information or to ask questions on what has occurred.

The DPO/IO will consider notifying third parties such as the police, insurers, banks or credit card companies, where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

Once the initial incident is contained, the DPO/IO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by Knoco Directors.

Social Media Policy

Knoco encourages the use of Social Media to raise the profile and reputation of the company, and to interact with potential collaborators, clients and customers. The Knoco social media policy applies to all official (Knoco-badged) social media channels, and all personal channels that contain postings about Knoco business, services, employers, customers, partners or competitors.

Requirements

The Knoco code of business ethics applies to all social media activity

The Knoco Information and data protection policy applies to all social media activity

You may not use social media to disclose Knoco confidential information, or confidential information about our clients or customers. All reference to clients and customers on social media must comply with any written confidentiality, publicity, or non-disclosure agreement signed with these clients. You may make observations about competitors' products and activities if your observations are accurate and based on publicly available information.

Do not disparage or denigrate competitors.

Do not publish (nor should you possess) our competitors' proprietary or confidential information.

Do not use copyright images in your publications without permission.

Wherever possible, make a clear distinction between Company social activity, and personal. For example, the Knoco Facebook page should be used for Knoco-related announcements and public discussion, while personal Facebook pages are used for personal discussion.

Any Knoco-related or franchisee-related social media channel primarily aimed at business should make this clear in the channel name or title (example, “Knoco Stories”). Any personal blogs which discuss Knoco business should bear the text *“The views expressed on this [blog; Web site] are my own and do not necessarily reflect the views of Knoco”*

Do not post anything that is false, misleading, obscene, defamatory, profane, discriminatory, libellous, threatening, harassing, abusive, hateful, or embarrassing to another person or entity. Make sure to respect others' privacy. Third party Web sites and blogs that you link to must meet our standards of propriety.

Don't Post Anonymously. While you are not an official spokesperson, your status as a Knoco member may still be relevant to the subject matter. You should identify yourself as affiliated to Knoco if failing to do so could be misleading to readers or viewers. Employees should not engage in covert advocacy for Knoco

Recognize and respect others' intellectual property rights, including copyrights. Never use more than a short excerpt from someone else's work, and make sure to credit and, if possible, link to the original source.

We will comply with any and all anti-spam legislation relevant to our place of business. The default is that we will not send any unsolicited marketing material, except where there is a clear exception provided by local legislation. All newsletters, electronic greetings cards and other such marketing material will be opt-in, which means that the recipient, if not a client to which we have delivered service within the last 2 years, must have agreed in advance to receive it (see e-Newsletter policy).

Quality Management Policy

Knoco commits to understand, meet and, when possible, exceed Customer's Requirements through the continuous improvement of our processes. We are dedicated to delivering defect-free product on-time at or below the agreed cost.

The Quality Management method applied by Knoco Ltd is linked to the Learning approach, and involves four main components;

1. Learning Before for Quality Assurance.

All work for clients, unless new work, will be based on existing quality standards and processes embedded in the most recent products. For example, all assessments will use the most recent assessment protocol, the most recent report format, and the most recent database. These documents are stored in the Knoco Wiki. Further guidance may be sought as appropriate from Knoco directors and consultants in the form of remotely assisted or face-to-face Peer Assists.

2. Director-level Quality Control

All reports for clients, all training and reference material, and all training agendas, will be checked by at least one Director for Quality Control purposes.

3. Lead consultant accountability.

The Knoco lead consultant is fully accountable for all Quality Assurance and Quality Control of project deliverables.

4. Client feedback.

Client feedback will be sought through regular progress reviews and end-of-stage retrospects with the client wherever possible. Actions arising from these reviews will be reviewed by the Knoco Directors, and the Knoco approach updated wherever necessary.

5. Updating Knoco knowledge base.

All new knowledge, new approaches, process improvements and other enhancements will be uploaded to the Knoco wiki. The Knoco Director, resources and training retains editorial rights to the Wiki, and will review and validate all updates.

6. Client Quality System.

The lead consultant will ensure that any Client Quality system is applied to the project in addition to the Knoco Quality Management approach.

Knowledge, Learning and Knowledge Management policy

The Knoco Learning and Knowledge Management policy is as follows;

1. Learning Before.

The Project Lead will consult the Knoco Wiki for the most up to date guidance on the processes and approaches to be used on the project. Further guidance may be sought as appropriate from Knoco directors and consultants in the form of remotely assisted or face-to-face Peer Assists.

2. Learning During.

Learning reviews, using an extended After Action Review format, should be held at all major milestones and deliverables, including steering team review meetings, or at an interval not greater than monthly. Actions arising from these reviews will be forwarded to the Directors for validation and updates made to the Knoco Wiki. Important updates will be circulated to the Knoco distribution list.

3. Learning After.

Project team Retrospects should be held at the end of each project or project stage. These reviews will compare anticipated delivery against actual delivery, and seek to identify learning points whenever actual deviates from expected. Lessons from these reviews will be used to improve the internal working process. These will be updated on the Knoco Wiki.

4. Knowledge Base

The Knoco wiki will act as our knowledge base. This contains validated guidance documents for our own use, training materials, reference materials, and examples of key output documents. All new knowledge, new approaches, process improvements and other enhancements will be uploaded to the Knoco wiki. The Knoco Director, resources and training retains editorial rights to the Wiki, and will review and validate all updates.

5. Community of Practice

The list of Knoco directors, franchisees and associates represents our community of practice. We will make use of the community should queries arise at any stage in our projects, using email, Skype and Skype conference, Yammer, discussion functionality on the Wiki (if appropriate), and any other available functionality.

6. Training.

Knoco Franchisees will be provided with induction training when joining the organisation. The individual training and development needs of Knoco staff, franchisees or associates will be identified on an annual basis, or depending on the needs of particular contracts. Learning

and development needs identified will be met through a variety of activities, including coaching and shadowing, depending on the nature and extent of the requirements. External courses and professional qualifications may be fully or partly funded by the organisation depending on the nature of the training. Knoco directors, employees and franchisees are responsible for their own development and as such may inform the organisation of their development needs and take part in prescribed development activities. This policy respects equal opportunities and applies to all Knoco directors, employees and franchisees.

HSE (Health, Safety and Environmental) Policy

Everybody who works for Knoco, anywhere, is responsible for getting HSE right. Good HSE performance and the health, safety and security of everyone who works for the Company are critical to the success of its business.

Knoco's HSE goals are simply stated:

- no accidents
- no harm to people
- no damage to the environment

Knoco will maintain the health and safety of its staff by effective management of travel and security risks, and through provision of travel insurance. Knoco franchisees are expected to maintain travel and health insurance when travelling out of their territory of work on Knoco business.

Knoco will continue to improve the environmental and impact of its operations by reducing waste, emissions and discharges, and by using energy efficiently. All leaders within the Company will be held accountable for accomplishing the HSE goals by demonstrating correct HSE behaviours, by providing needed resources and by measuring, reviewing and continuously improving our HSE performance.

In addition, Knoco directors, staff, associates and franchisees will abide by client HSE policies when working for any particular client.

Code of Business Ethics

Knoco directors, staff, franchisees (on Knoco business) and sub contractors to Knoco will be bound by and will display the highest possible standards of business ethics. We recognise our obligation to society and the world in which we live.

We will not be involved in;

- illegal activities
- offering bribes or inducements to client representatives nor will we allow agents acting on our behalf to offer bribes or inducements (any gifts to clients must not exceed £40 in value)
- financial record keeping or payments that do not comply with the guidance provided by the appropriate professional institutions

- poaching staff from other organisations
- selling or marketing material from client organisations that we are not entitled to
- industrial espionage on behalf of any organisation or government
- any activities which undermine the human rights of the individual
- price fixing cartels or any trade organisation that do not support free trade.

We respect the rights of the individual and the intellectual property rights of companies.

The directors of Knoco will monitor for non compliance, and will discuss any potential situation that might arise which would challenge our Code of Ethics. We will then proactively manage the situation. Each director, franchisee and associate is required to verify that they have not breached the code of ethics.

Equal opportunities policy

This organisation aims to ensure that no job applicant or worker receives less favourable treatment on the grounds of race, colour, gender orientation, nationality, religion, ethnic or national origin, age, gender, gender reassignment or marital status, sexual orientation or disability. There will be no discrimination on these grounds in the terms and conditions offered to workers or job applicants. Selection criteria and procedures are reviewed to ensure that individuals are treated on the basis of their relevant merits and abilities. All workers will be given equal opportunity and access to training to enable them to progress both within and outside the organisation. The policy also covers recruitment, induction, conduct at work and the disciplinary and grievance procedure. The only basis for promotion or selection is the management's considered opinion of the applicant's suitability for the job. All workers have a legal and moral obligation not to discriminate and to report incidents of discrimination against any individual or group of individuals. Any worker found to be discriminating will face disciplinary proceedings.