KNOX & WELLS LTD

GDPR POLICIES

This document includes the following policies:

- Data Protection Policy
- Email Use Policy
- Internet Use Policy
- Social Media Policy
- Website Privacy Policy

DATA PROTECTION POLICY

CONTEXT & OVERVIEW

Key Details:

- Policy prepared by: *Sophie Leach*
- Approved by board/management on: *23/05/2018*
- Policy became operational on: *25/05/2018*
- Next Review Date: *25/05/2019*

Introduction

Knox & wells needs to gather and use certain information about individuals.

These can include customers, suppliers, subcontractors, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures Knox & Wells:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations – including Knox & Wells – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date

5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

PEOPLE, RISKS & RESPONSIBILITIES

Policy Scope

This policy applies to:

- The head office of Knox & Wells
- All site locations of Knox & Wells
- All Staff and volunteers of Knox & Wells
- All contractors, suppliers and other people working on behalf of Knox & Wells

Its applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of the individuals
- Postal Addresses
- Email Addresses
- Telephone Numbers
- …plus, any other information relating to individuals

Data Protection Risks

This policy helps to protect Knox & Wells from some very real data security risks including:

- ***Breaches of Confidentiality***. For instance, information being given out inappropriately.

- ***Failing to offer choice***. For instance, all individuals should be free to choose how the company uses data relating to them.
- ***Reputational Damage***. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Knox & Wells has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Knox & Wells meets its legal obligations.
- The Data Protection Officer (*Adrian Lewis*), is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Knox and Wells holds about them (also called 'subject access requests')
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The IT Manager (*Sophie Leach*), is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing service.
- The Marketing Manager (*Sophie Leach*), is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those **who need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it form their line managers.
- Knox and wells **will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.

- Personal Data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data print outs should be shredded** and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD) these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers and** should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in secure location**, away from general office space.
- Data should be **backed up frequently.** Those backups should be tested regularly, in line with the company standard back up procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

DATA USE

Personal data is of no value to Knox & Wells unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure their screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

DATA ACCURACY

The law requires Knox & Wells to take reasonable steps to ensure data is kept accurate and up to data.

The more important it is that the personal data is accurate, the greater the effort Knox & Wells should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Knox & Wells will make it easy for **data subjects to update the information** Knox & Wells hold about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by Knox & Wells are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at (email address). The data controller can supply a standard request for, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

SUBJECT ACCESS REQUESTS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances Knox & Wells will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

PROVIDING INFORMATION

Knox & Wells aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

(This is available on request. A version of this statement is also available on the company's website.]

EMAIL USE POLICY

CONTEXT & OVERVIEW

Key Details:

- Policy prepared by: *Sophie Leach*
- Approved by board/management on: *23/05/2018*
- Policy became operational on: *25/05/2018*
- Next Review Date: *25/05/2019*

Introduction

Knox & Wells makes email available to its employees where relevant and useful for their jobs.

This email use policy describes the rules governing email use at the company. It also sets out how staff members are expected to behave when using email.

This policy should be read alongside other key policies. In particular, users should also read the company's data protection and internet use policies.

Why this policy exists

Email is a standard way to communicate in business. It's used widely and is arguably just as important as the telephone.

Like any technology, email can cause difficulties if used incorrectly or inappropriately. This email policy:

- Reduces the security and business risks faced by Knox & Wells.
- Let's staff know how they are permitted to use company email.
- Ensures employees follow good email etiquette
- Helps the company satisfy its legal obligations

POLICY SCOPE

This policy applies to all staff, contractors and volunteers at Knox & Wells who use the company email system.

It applies no matter where that email use takes place: on company premises, while travelling for business or while working from home.

It applies to use of company email on any device, no matter whether owned by the company or employee.

Business Email Use

Knox & Wells recognises that email is a key communication tool. It encourages it employees to use email whenever appropriate.

For instance, staff members may use email to:

- Communicate with customers or suppliers
- Market the company's products
- Distribute information to colleagues

Personal Email Use

The company also recognises that email is an important tool in many people's daily lives. As such it allows employees to use their company email account for personal reasons, with the following stipulations:

- Personal email use should be if a reasonable level and restricted to non-work times, such as breaks and during lunch.
- All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate no matter whether it is being sent or received for business or personal reasons.
- Personal email use must not affect the email service available to other users. For instance, sending exceptionally large files by email could slow access for other employees.
- Users may access their own personal email accounts at work, if they do so via our internet connection. For instance, a staff member may check their Yahoo or Google Mail during their lunch break.

Authorised Users

Only people who have been authorised to use email at Knox & Wells may do so.

Authorisation is usually provided by an employee's line manager or the company IT department. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

Unauthorised use of the company's email system is prohibited.

Employees who use company email without authorisation – or who provide access to unauthorised people – may have disciplinary action taken against them.

KEY AREAS

Email Security

Used inappropriately, email can be a source of security problems for the company. Users of the company email system must not:

- Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.
- Disable security or email scanning software. These tools are essentials to protect the business from security problems.

- Send confidential company data via email. The IT department can advise on appropriate tools to use instead.
- Access another user's company email account. If they require access to a specific message (for instance, while an employee is off sick), they should approach their line manager or the IT department.

Staff members must always consider the security of the company's systems and data when using email. If required, help and guidance is available from line managers and the company IT department.

Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception.

Although such interceptions are rare, it's best to regard email as an open communication system, not suitable or confidential messages and information.

Inappropriate email consent and use

The company email system must not be used to send or store inappropriate content or materials.

It is important employees understand that viewing or disturbing inappropriate content via email is not acceptable under any circumstances.

Users must not:

- Write or send emails that might be defamatory or incur liability for the company.
- Create or distribute any inappropriate content or material via email.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text or images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use email for any illegal or criminal activates.
- Send offensive or harassing emails to others.
- Send messages or material that could damage Knox & Wells' image or reputation.

Any user who receives an email they consider to be inappropriate should report this to their line manager or supervisor.

Copyright

Knox & Wells respects and operates within copyright laws. Users may not use company email to share copyrighted software, media or materials owned by third parties, unless permitted but that third party.

Employees must not use the company's email system to perform any tasks that may involve breach of copyright law.

Users should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright.

Contracts and Liability

Users must be careful about making commitments or agreeing to purchases via email.

An email message many form a legally-binding contract between Knox & Wells and the recipient even if the user has not obtained proper authorisation within the company.

Email Disclaimer

The standard company email template includes an email disclaimer. Users must not remove or change this when they send messages.

Email Marketing and Bulk Email

Knox & Wells may use email to market to existing and potential customers.

There is significant legislation covering bulk email and use of email for marketing.

All email campaigns must be authorised by the marketing manager and implemented using a suitable email marketing tool.

Users must not send bulk emails using the standard business email system.

All questions about email marketing should be directed to the marking manager.

EMAIL BEST PRACTICE

Email Etiquette

Email is often used to communicate with customers, partners and other important contacts. Although a relatively informal medium, staff should be aware that each email they send does affect the company's image and reputation.

It's a good idea to follow rules of good email etiquette. Users must:

- Not forward on chain emails or 'humorous' messages. These clogs up people's in-boxes and some topics are not appropriate for the workplace.
- Always use a meaningful subject line rather than leaving it blank or using a single word like 'hello'.
- Only use the 'important message' setting sparingly, for messages that really are important.
- Never ask recipients to send a 'message read' receipt. Many people find these annoying and not all email services support them.
- Do not use ALL CAPITAL LETTERS in messages or subject lines. This can be perceived as impolite.
- Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful.
- Use the 'CC' (carbon copy) field sparingly. If someone really needs to receive a message, they should be included in the 'to' field.

- Use the 'BCC' (blind carbon copy) field to send group messages where appropriate. It stops an email recipient seeing who else was on the email.

Internal Email

Email is a valid way to communicate with colleagues. However, it tends to be overused for internal communication.

Users should keep these points in mind when emailing colleagues:

- Would the issue be better addressed via a face-to-face discussion or telephone call?
- Is email the best way to send a document out for discussion? Often, it becomes very hard to keep track of feedback and versions.
- It's rarely necessary to 'reply all'. Usually, it's better to reply and then manually add other people who need to see a message.

POLICY ENFORCEMENT

Monitoring Email Use

The company email system and software are provided for legitimate business use.

The company therefore reserves the right to monitor employee use of email.

Any such examinations of monitoring will be carried out by authorised staff.

Additionally, all emails sent or received through the company's email system are part of official Knox & Wells records. The company can be legally compelled to show that information to law enforcement agencies or other parties.

Users should always ensure that the business information sent via email is accurate, appropriate, ethical and legal.

Potential Sanctions

Knowingly breaching this email use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employee, contractors and others users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breeches of this policy.

However, the company is unlikely to take formal action if a user fails to adhere to the guidelines in the 'email best practice' section.

INTERNET USE POLICY

CONTEXT & OVERVIEW

Key Details:

- Policy prepared by: *Sophie Leach*
- Approved by board/management on: *23/05/2018*
- Policy became operational on: *25/05/2018*
- Next Review Date: *25/05/2019*

Introduction

Knox & Wells makes internet access available to its employees where relevant and useful for their jobs.

This internet use policy describes the rules governing internet use at the company. It also sets out how staff members are expected to behave when using the internet.

This policy should be read alongside other key policies. The company's data protection and email policies are particularly relevant to staff who use the internet.

Why this policy exists

The internet is a powerful tool that can bring significant benefits to Knox & Wells.

However, it's important every person at the company who uses the internet understands how to use it responsibly, safely and legally.

The internet use policy:

- Reduces the **online security risks** faced by Knox & Wells
- Let staff know what they **can and can't do** online
- Ensures employees **do not view inappropriate content** at work
- Helps the company **satisfy its legal obligations** regarding internet use

Policy Scope

It applies no matter whether that internet access takes place on company premises, while travelling for business or while working from home.

It applies to use of the internet on any device that is owned by the company, or that is connected to any company networks or systems.

For example, it applies both to an employee using the internet at their desk, staff on site connecting to wireless routers and to employees who connect their own tablets or smart phones to the company wireless network.

GENERAL INTERNET GUIDELINES

Internet use is encouraged

Knox & Wells recognises that the internet is an integral part of doing business. It therefore encourages its employees to use the internet whenever such use supports the company goals and objectives.

For instance, staff members may use the internet to:

- Purchase office supplies
- Book business travel
- Perform competitor or market research
- Identify potential suppliers or partners

There are many valid reasons for using the internet at work and the company certainly allows its employees to explore and make use of the internet's many advantages.

Personal Internet Use

The company also recognises that the internet is embedded in many people's daily lives. As such, it allows employees to use the internet for personal reasons, with the following stipulations:

- Personal internet use should be a reasonable level and restricted to non-work times, such as breaks and during lunch.
- All rules described in this policy apply equally to personal internet use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.
- Personal internet use must not affect the internet service available to other people in the company. For instance, downloading large files could slow access for other employees.

Authorised Users

Only people who have been authorised to use the internet at Knox & Wells may do so.

Authorisation is usually provided by an employee's line manager or the company IT department. It id typically granted when a new employee joins the company and is assigned their IT login details for the company IT systems.

Unauthorised use of the internet without authorisation – or who provide access to unauthorised people – may have disciplinary action taken against them.

KEY AREAS

Internet Security

Used unwisely, the internet can be a source of security problems that can do significant damage to the company's data and reputation.

- Users must not knowingly introduce any form of computer virus, Trojan, spyware or other malware into the company.

- Employees must not gain access to websites or systems for which they do not have authorisation, either within the business or outside it.
- Company data should only be uploaded to and shared via approved services. The IT department can advise on appropriate tools for sending and sharing large amounts of data.
- Employees must not steal, use or disclose someone else login or password without authorisation.

Staff members must always consider the security of the company's systems amd data when using the internet. If required, help and guidance is available from the line managers and the company OT department.

Inappropriate content and uses

There are many sources of inappropriate content and materials available online. It is important for employees to understand that viewing or distributing inappropriate content is not acceptable under any circumstances.

Users must not:

- Take part in any activities on the internet that could bring the company into disrepute.
- Create or transmit material that might be defamatory or incur liability for the company.
- View, download, create or distribute any inappropriate content or material.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use the internet for any illegal or criminal activity
- Send offensive or harassing material to others
- Broadcast unsolicited personal views on social, political, religious or other non-business related matters.
- Send or post messages or material that could damage Knox & Wells' image or reputation.

Copyright

Knox & Wells respects and operates within copyright laws. Users may not use the internet to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
- Download illegal copies of music, films, games or other software, whether via filesharing services or other technologies.

POLICY ENFORCEMENT

Monitoring Internet Use

Company IT and internet resources – including computers, smart phones and internet connections – are provided for legitimate business use.

The company therefore reserves the right to monitor use of the internet, to examine systems and review the data stored in those systems.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all internet data written, sent or received through the company's computer systems is part of official Knox & Wells records. The company can be legally compelled to show that information to law enforcement agencies or other parties.

Users should always ensure that the business information sent over or uploaded to the internet is accurate, appropriate, ethical and legal.

Potential Sanctions

Knowingly breaching this internet use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

SOCIAL MEDIA POLICY

CONTEXT & OVERVIEW

Key Details:

- Policy prepared by: *Sophie Leach*
- Approved by board/management on: *23/05/2018*
- Policy became operational on: *25/05/2018*
- Next Review Date: *25/05/2019*

Introduction

Social media can bring significant benefits to Knox & Wells, particularly for building relationships with current and potential customers.

However, it's important that employees who use social media within the company do so in a way that enhances the company's prospects.

A misjudged status update can generate complaints or damage the company's reputation. There are also security and data protection issues to consider.

This policy explains how employees can use social media safely and effectively.

Policy Scope

This policy applies to all staff, contractors and volunteers at Knox & Wells who use social media while working – no matter whether for business or personal reasons.

It applies no matter whether that social media use takes place on company premises, while travelling for business or while working from home.

Social Media sites and services include (but are not limited to):

- Popular social networks like **Twitter** and **Facebook**
- Online review websites like **Reevo** and **Trustpilot**
- Sharing and discussion sites like **Delicious** and **Reddit**
- Photographic social networks like **Flickr** and **Instagram**
- Question and answer social networks like **Quora** and **Yahoo Answers**
- Professional social networks like **LinkedIn** and **Sunxu**.

Responsibilities

Everyone who operates a company social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

However, these people have key responsibilities:

- The social media manager (*Sophie Leach*) is ultimately responsible for ensuring that Knox & Wells uses social media safely, appropriately and in line with the company's objectives.
- The IT manager (*Sophie Leach*) is responsible for providing apps and tools to manage the company's social media presence and track any key performance indicators. They are also responsible for proactively monitoring for social media security threats.
- The marketing manager (*Sophie Leach*) is responsible for working with the social media manager to roll out marketing ideas and campaigns through our social media channels.
- The customer service manager is responsible for ensuring requests for assistance and support made via social media are followed up.

GENERAL SOCIAL MEDIA GUIDELINES

The power of social media

Knox & Wells recognises that social media offers a platform for the company to perform marketing, stay connected with customers and build its profile online.

The company also believes its staff should be involved in industry conversations on social networks. Social media is an excellent way for employees to make useful connections, share ideas and shape discussions.

The company therefore encourages employees to use social media to support the company's goals and objectives.

Basic Advice

Regardless of which social networks employees are using, or whether they're using business or personal accounts on company time, following these simple rules helps avoid the most common pitfalls:

- **Know the social network.** Employees should spend time becoming familiar with the social network before contributing. It's important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.
- **If unsure, don't post it.** Staff should err on the side of caution when posting on social networks. If an employee feels an update pr message might cause complaints or offence – or be otherwise unsuitable – they should not post it. Staff members can always consult the social media manager for advice.
- **Be thoughtful and polite.** Many social media users have got into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email.
- **Look out for security threats.** Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.

- **Keep personal use reasonable.** Although the company believes that having employees who are active on social media can be valuable both to those employees and to the business, staff should exercise restraint in how much personal use of social media they make during working hours.
- **Don't make promises without checking.** Some social networks are very public, so employees should not make any commitments or promises on behalf of Knox & Wells without checking that the company can deliver on the promises. Direct any enquiries to the social media manager.
- **Handle complex queries via other channels.** Social networks are not a good place to resolve complicated enquiries and customer issues. Once a customer has made contact, employees should handle further communications via the most appropriate channel – usually email or telephone.
- **Don't escalate things.** It's easy to post a quick response to a contentious status update and then regret it, Employees should always take the time to think before responding, and golf back if they are in any doubt at all.

USE OF COMPANY SOCIAL MEDIA ACCOUNTS

This part of the social media policy covers all use of social media accounts owned and run by the company.

Additional Users

Only people who have been authorised to use the company's social networking accounts may do so.

Authorisation is usually provided by the social media manager. It is typically granted when social media-related tasks form a core part of an employee's job.

Allowing only designated people to use the accounts ensures the company's social media presence is consistent and cohesive.

Creating social media accounts

New social media accounts in the company's name must not be created unless approved by the social media manager.

The company operates its social media presence in line with a strategy that focuses on the most appropriate social networks, given available resources.

If there is a case to be made for opening a new account, employees should raise this with the social media manager.

Purpose of company social media accounts

Knox & Wells' social media accounts may be used for many different purposes.

In general, employees should only post updates, messaged or otherwise use these accounts when that use is clearly in line with the company's overall objectives.

For instance, employees may use company social media accounts to:

- Respond to customer enquiries and requests for help
- Share blog posts, articles and other content created by the company
- Share insightful articles, videos, media and other content relevant to the business, but created by others.

- Provide fans or followers with an insight into what goes on at the company
- Promote marketing campaigns and special offers
- Support new product launches and other initiatives

Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it, and to put those ideas to the social media manager.

Inappropriate content and uses

Company social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the company into disrepute.

When sharing an interesting blog post, article or piece of content, employees should always review the content thoroughly, and should not post a link based solely on a headline.

Further guidelines can be found below.

USE OF PERSONAL SOCIAL MEDIA ACCOUNT AT WORK

The value of Social Media

Knox & Wells recognises that employees' personal social media accounts can generate a number of benefits. For instance:

- Staff members can make **industry contacts** that may be useful for their jobs.
- Employees can discover content to help them **learn and develop** in their role
- By posting about the company, staff members can help to **build the business profile** online

As a result, the company is happy for employees to spend a reasonable amount of time using their personal social media accounts at work.

Personal social media rules

Acceptable use:

- Employees may use their personal social media for accounts **for work-related purposes** during regular hours, but must ensure this is for a **specific reason** (e.g. Competitor research). Social media should not affect the ability of employees to perform their regular duties.
- Use of social media accounts for non-work purposes is **restricted to non-work times**, such as breaks and during lunch.

Talking about the company:

- Employees should ensure it is clear that their social media account **does not represent Knox & Wells' views or opinions.**
- Staff may wish to include a disclaimer in social media profiles: 'The views expressed are my own and do not reflect the views of my employer.'

SAFE, RESPONSIBLE SOCIAL MEDIA USE

The rules in this section apply to:

- Any employees using company social media accounts
- Employees using personal social media accounts during company time

Users must not:

- Create or transmit material that might be defamatory or incur liability for the company.
- Post message, status updates or links to material or content that is inappropriate

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use social media for any **illegal or criminal activities**
- Send **offensive or harassing material** to others via social media
- Broadcast unsolicited views on social, political, religious or other non-business related matters
- Send or post messages or material that **could damage Knox & Wells' image or reputation**.
- Interact with Knox & Wells' competitors in any ways which could be interpreted as being **offensive, disrespectful or rude.** (Communication with direct competitors should be kept to a minimum.)
- Discuss **colleagues, competitors, customers or suppliers** without their approval
- Post, upload, forward or link to **spam, junk email or chain emails and messages**.

Copyright

Knox & Wells respects and operates within copyright laws. Users may not use social media to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party

  If staff wish to share content published on another website, they are free to do so if that website has obvious sharing buttons or functions on it.
- Share links to illegal copies of music, films, games or other software.

Security and Data Protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

- Maintain confidentiality

  Users must not:

  - Share or link to any content or information owned by the company that could be considered confidential or commercially sensitive.

    This might include sales figures, details of key customers, or information about future strategy or marketing campaigns.

  - Share or link to any content or information owned by another company or person that could be considered confidential or commercially sensitive.

    For example, if a competitors marketing strategy was leaked online, employees of Knox & Wells should not mention it on social media.

  - Share or link to data in any way that could breach the company's data protection policy.

- Protect Social Accounts

  - Company social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.

  - Wherever possible, employees should use two-factor authentication (often called mobile phone verification) to safeguard company accounts.

  - Staff must not use a new piece of software, app or service with any of the company's social media accounts without receiving approval from the social media manager.

- Avoid social scams

  - Staff should watch for phishing attempts, where scammers may attempt to use deception to obtain information relating to either the company or its customers.

    Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.

  - Employees should avoid clicking links in posts, updates and direct messages that look suspicious. In particular, users should look out for URLS contained in generic or vague-sounding direct messages.

POLICY ENFORCEMENT

Monitoring social media use:

Company IT ad internet resources – including computers, smart phones and internet connections – are provided for legitimate business use.

The company therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all data relating to social networks written, sent or received through the company's computer systems is part of official Knox & Wells records.

The company can be legally compelled to show that information to all enforcement agencies or other parties.

Potential Sanctions

Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and others users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

WEBSITE PRIVACY POLICY

KEY DETAILS

This website privacy policy describes how Knox & Wells protects and makes use of information you give the company when you use its website.

If you are asked to provide information when using this website, it will only be used in the ways described in this privacy policy.

This policy is updated from time to time. The latest version is published on this page.

The website privacy policy was updated on:

If you have any questions about this policy, please email info@knoxandwells.com or write to Knox & Wells Ltd, Creswell House, Fieldway, Cardiff, CF14 0RA.

INTRODUCTION

We gather and use certain information about individuals in order to provide products and services and to enable certain functions on our website.

We also collect information to better understand how visitors use our website and to present timely relevant information to them.

WHAT DATA WE GATHER

We may collect the following information:

- Name & Job Title
- Contact information including email address
- Demographic information, such as postcode, preferences and interests
- Website usage data
- Other information relevant to client enquiries
- Other information pertaining to special offers and surveys

HOW WE USE THIS DATA

Collecting this data helps us understand what you are looking for from the company, enabling us to deliver improved products and services.

Specifically, we may use data:

- For our own internal records
- To improve the products and services we provide
- To contact you in response to a specific enquiry
- To customise the website for you
- To send you promotional emails about products, services, offers and other things we think might be relevant to you.
- To send you promotional mailings or to call you about products, services, offers and other things we think might be relevant to you
- To contact you via email, telephone or mail for market research reasons.

COOKIES AND HOW WE USE THEM

What is a cookie?

A cookie is small file placed on your computer's hard drive. It enables our website to identify your computer as you view different pages on our website.

Cookies allow websites and applications to store your preferences in order to present content, options or functions that are specific to you. They also enable us to see information like how many people use the website and what pages they tend to visit.

How we use cookies?

We may use cookies to:

- **Analyse our web traffic using an analytics package.** Aggregated usage data helps us improve the website structure, design content and functions.

- **Identify whether you are signed in to our website.** A cookie allows us to check whether you are signed in to the site.
- **Test content on our website.** For example, 50% of our users might see one piece of content, the other 50% a different piece of content.
- **Store information about your preferences.** The website can then present you with information you will find more relevant and interesting.
- **To recognise when you return to our website.** We may show your relevant content, or provide functionality you used previously.

Cookies do not provide us with access to your computer or any information about you, other than that which you choose to share with us.

Controlling cookies

You can use your web browser's cookie settings to determine how our website uses cookies. If you o not want our website to store cookies on your computer or device, you should set your web browser to refuse cookies.

However, please note that doing this may affect how our website functions. Some pages and services may become unavailable to you.

Unless you have changed your browser to refuse cookies, our website will issue cookies when you visit it.

To learn more about cookies and how they are used, visit the All About Cookies website at www.allaboutcookies.org

CONTROLLING INFORMATION ABOUT YOU

When you fill in a form or provide your details on our website, you will see one or more tick boxes allowing you to:

- Opt-in to receive marketing communications from us by email, telephone, text message or post.
- Opt-in to receive marketing communications from our third-party partners by email, telephone, text messages or post

If you have agreed that we can use your information for marketing purposes, you can change your mind easily, via one of these methods:

- Sign in to or website and change your opt-in settings, if applicable
- Send an email to: info@knoxandwells.com
- Write to us at: Knox & Wells Ltd, Creswell House, Fieldway, Cardiff, CF14 4UH

We will never lease, distribute or sell your personal information to third parties unless we have your permission or the law requires us to.

Any personal information we hold about you is stored and processed under our data protection policy in line with the Data Protection Act 1998.

SECURITY

We will always hold your information securely.

To prevent unauthorised disclosure or access to your information, we have implemented strong physical and electronic security safeguards.

We also follow stringent procedures to ensure we work with all personal data in line with the Data Protection Act 1998.

LINKS FROM OUR SITE

Our website may contain links to other websites.

Please note that we have no control of websites outside the knoxandwells.com domain. If you provide information to a website to which we link, we are not responsible for its protection and privacy.

Always be wary when submitting data to websites. Read the site's data protection and privacy policies fully.