**Tudor Rose**
**Information and Communications Technology Policy**
May 2018

**Contents**

## 1. Introduction

Information and communications technology (ICT) is provided by Tudor Rose for employees to use in fulfilling their business roles. All ICT use is governed by the rules and procedures set out in the terms of this policy.

At Tudor Rose, communication with colleagues, clients and business partners plays an essential role in the conduct of our business. How you communicate with other individuals reflects both upon you as a person and Tudor Rose as an organisation.

We invest substantially in ICT and to enable you to work more effectively, and expect you to use ICT responsibly and appropriately.

Please read this entire policy carefully. If the terms of this policy are not adhered to, your use of ICT may be curtailed or withdrawn, and you may be subject to disciplinary action.

## 2. Definitions

“ICT” refers to any communications device, application or service, including: fixed line and mobile telephones, laptop, desktop and tablet computers, applications, whether installed on a device or accessed via the internet, such as those within Microsoft Office, Microsoft Dynamics CRM and Adobe software, e-mail and other messaging services, radio, television, network and server hardware and software.

“User” refers to any person who accesses an ICT system or service owned, managed or supplied by Tudor Rose.

“Network” refers to any data communications links such as ethernet, wireless or fibre at Tudor Rose offices or provided by Tudor Rose via the internet.

**3. Relevant Laws and Regulations**

It is the policy of Tudor Rose that all activities must be conducted within current regulation.

The use of information and communications technology is governed by a variety of different Acts of Parliament. These currently include:

- Privacy and Electronic Communications Regulations 2003
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
- The Copyright, Designs and Patents Act 1988
- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Human Rights Act 1998
- The Regulation of Investigatory Power Act 2000
- The Freedom of Information Act 2000
- The Electronic Communications Act 2000
- The Digital Economy Act 2010.
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

The ICT Manager has responsibility for monitoring legislation and when required making appropriate updates to the ICT Policy.

**4. ICT Policy Management**

4.1 All users must comply with the policy. Failure to do so may render employees liable to disciplinary action which could, in serious cases, lead to dismissal from their employment.

4.2 Breaches of any section of this policy are potentially disciplinary issues which may be handled in line with company disciplinary procedures.

4.3 Any suspicion of breach of the policy must be reported to the ICT Manager and your line manager immediately. Failure to do constitutes a breach of the policy.

4.4 The ICT Manager can suspend access to any accounts affected by a breach in the ICT Policy.

4.5 Tudor Rose is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. Tudor Rose may monitor your business communications for reasons which include:

4.5.1 Providing evidence of business transactions.

4.5.2 Ensuring that Tudor Rose's business procedures, policies and contracts with staff are adhered to.

4.5.3 Complying with any legal obligations.

4.5.4 Monitoring standards of service, staff performance, and for staff training.

4.5.5 Preventing or detecting unauthorised use of Tudor Rose's ICT or criminal activities.

4.5.6 Maintaining the effective operation of Tudor Rose's communication systems.

4.6 Tudor Rose will monitor telephone, e-mail, internet and social media data (e.g. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). This will be administered by and managed by the ICT Department within General Data Protection Regulation (GDPR).

4.5. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. By carrying out such activities using Tudor Rose's facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

4.7 Sometimes it is necessary for Tudor Rose to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the permission of your line manager or a Director.

4.8 Any e-mails which are not stored in a folder named 'Personal' in your mailbox are considered business communications since we have no way of knowing that they were intended to be personal. Furthermore, there is a risk that any person authorised to access your mailbox may have their own preview pane option as a default setting, which would reveal the content of any of your personal e-mail not filed in your 'Personal' folder. Therefore, as a provision for when you are out of the office, you may wish to set up a rule to automate the routing of personal e-mail to your personal folder – ask the ICT department for guidance on how to do this. It is up to you to prevent the inadvertent disclosure of the content of personal e-mail by filing your personal e-mail in accordance with this policy. In particular, you are responsible to anybody outside Tudor Rose who sends to you, or

receives from you, a personal e-mail, for the consequences of any breach of their privacy which may be caused by your failure to file your personal e-mail.

4.9 In certain very limited circumstances we may, subject to compliance with any legal requirements, access e-mail or folders marked ‘Personal’. Examples are when we have reasonable suspicion that they may reveal evidence of unlawful activity, including instances where there may be a breach of a contract with Tudor Rose or serious breach of policies including this ICT policy.

4.10 In cases where investigation of traffic or content of user accounts is necessary then the ICT Manager will carry out such work following authorisation from Human Resources or a Director. Tudor Rose will involve the police in all cases where they believe illegal activity has taken place.

4.11 Employees may be blocked from accessing certain websites during work hours/while connected to the network at the discretion of the company.

4.12 All incoming e-mails are scanned by using virus-checking software. The software will also attempt to block unsolicited marketing e-mail (spam), banned keywords and e-mails which have potentially inappropriate attachments. Inform the ICT Manager if you would like any e-mails you are receiving to be blocked, or require any further guidance on dealing with spam.

4.13 Existing users of ICT will be notified of this policy and future changes. The users’ continued use of ICT after notification will constitute acceptance and agreement to the policy document.

4.14 Future employees will be notified of the policy when they sign their contract of employment and will only be granted access to Tudor Rose systems and equipment once they have signed to accept this policy.

4.15 The ICT Manager will ensure this policy is reviewed annually to reflect best practice with revisions being approved by Human Resources and Directors.

**5. ICT Usage Guidelines**

5.1 Tudor Rose ICT must be used lawfully, responsibly and appropriately. Examples of inappropriate use of ICT include accessing, creating, sending and forwarding content of the following nature:

5.1.1 Pornographic, obscene, indecent or sexually explicit material.

5.1.2 Offensive, harassing, sexist, racist, hateful or otherwise discriminatory material.

5.1.3 Chain messages and jokes.

5.1.4 Private commercial activities.

5.1.5 Any form of defamation, discrimination, harassment or bullying.

5.1.6 The introduction of viruses, spyware or malware.

5.1.7 Causing harm to or bringing disrepute to Tudor Rose, a customer, business partner or colleague.

5.1.8 Representing personal opinions as that of the company.

5.1.9 Where it interferes with/impedes the business of Tudor Rose.

5.1.10 Where it misuses personal data of employees, clients or business partners.

5.2 Users must not in any way cause any form of damage to any Tudor Rose ICT. The term damage includes modifications to hardware, software or infrastructure which whether or not causing harm to the hardware or software, incur time and/or cost in restoring the system to its original state.

5.3 All software and hardware upgrades, moves and repairs are to be performed by, or under the direct supervision of, the ICT Manager. All damages, breakdowns or malfunctions are to be reported to the ICT Manager.

5.4 Users must comply with the terms of conditions of all licence agreements relating to any ICT related hardware, software or services.

5.5 User must not introduce any virus, worm, malware, Trojan horse and other nuisance program or file onto any system.

5.6 Users may only access files they have created and files they have been given express permission to access.

5.7 Users must not connect any equipment, including personal mobile phones, to the Company's network without prior authority from the ICT Manager.

5.8 Users must not allow any password associated with his/her username to become known to another user. Users will be held responsible for any unlawful action carried out under his/her computer account unless there is evidence to prove otherwise.

5.9 Users must not make known any other passwords which may be supplied to them in to enable access to Tudor Rose ICT.

5.10 If leaving devices unattended in Tudor Rose offices, users must ensure that they are password protected.

5.11 Do not leave devices unattended when out of the office, unless adequately secured, for example locked at home or in a hotel room or locked and out of sight in a vehicle. Do not store devices in a vehicle overnight.

5.12 Users must not download or install any applications without the express prior permission of their line manager and the ICT Manager.

5.13 Lost or stolen devices must be reported to your line manager and the ICT Manager within 24 hours.

5.14 Users must not engage in any unlawful activity using Tudor Rose ICT.

**6. E-mail, Internet and Social Media usage**

6.1 Users sending e-mail from any Tudor Rose domain (e.g. @tudor-rose.co.uk, @cruiseandferry.net, @technologyrecord.com or @golfcoursearchitecture.net), posting Internet content or conducting social media activity on behalf of Tudor Rose should act in an appropriate and responsible manner.

6.2. Never reply to any Spam or Phishing emails or access links provided within such e-mails. Spam email is unsolicited email, often referred to as 'junk' email and is often indiscriminately sent to multiple email addresses, usually inviting you to purchase a product or service. Phishing is an attempt to fraudulently acquire sensitive or person identifiable information like credit card details, bank account details, passwords or other similar information, usually by masquerading as a trustworthy source, such as a bank.

6.3 Consider bandwidth implications when adding attachments to e-mail messages. If you need to transmit files in excess of 20MB consult with the ICT Manager to decide upon the most effective means of transmission.

6.4 Exercise good practice with e-mail use to ensure that it isn't disruptive to your work or that of your colleagues, clients and business partners. Avoid sending unnecessarily long messages and pay specific consideration to whether recipients should be on the To: line (generally meaning action is required) or Cc: line (generally meaning for information only).

6.5 Do not send personal emails to large numbers of recipients.

6.6 Do not use e-mail in a manner that is similar to instant messaging.

6.7 Do not stream radio, music and video services via the Tudor Rose network unless directly related to your job role.

6.8 Only those persons officially designated by Tudor Rose have the authorisation to represent the company on company-created web pages, social media pages or other web pages and social media pages. The ICT Manager owns the list of users and groups authorised to represent the company.

6.9 The following are policy guidelines regarding what you should and should not do when publishing content on the web and in social media. These guidelines apply to all web and social media publishing, whether personal or company-owned. Employees are responsible for content they publish in social media and can be held personally liable for content published. Employees can also be subject to disciplinary action by Tudor Rose for publishing inappropriate, confidential content or content that damages the reputation of Tudor Rose, a customer, business partner or colleague. These guidelines only cover a sample of all possible content publishing scenarios and are not a substitute for good judgment.

> 6.9.1 Understand and follow all privacy and confidentiality guidelines in the Tudor Rose Company Handbook. All guidelines in the handbook, as well as laws such as copyright, fair use and financial disclosure laws apply to internet and social media use.
>
> 6.9.2 Do not disclose or use Tudor Rose confidential or proprietary information or that of any other person or company. For example, ask permission before posting someone's picture in a social network or publishing in a blog a conversation that was meant to be private.
>
> 6.9.3 Do not comment on Tudor Rose's confidential financial information such as future business performance or business plans.
>
> 6.9.4 Do not cite or reference customers, partners or suppliers without their written approval

Some individuals work anonymously, using pseudonyms or false screen names. Tudor Rose discourages that practice.

6.9.5 If you have identified yourself as a Tudor Rose employee within a social website, you are connected to your colleagues, managers and even Tudor Rose customers. You should ensure that content associated with you is consistent with your work at Tudor Rose.

6.9.6 Ask permission – to publish or report on conversations that are meant to be private or internal to Tudor Rose and when in doubt, always ask permission from a Director.
6.9.7 Speak in the first person when engaging in personal internet and social media communications. Make it clear that you are speaking for yourself and not on behalf of Tudor Rose.

6.9.8 If you publish personal internet and social media communications and it has something to do with the work you do or subjects associated Tudor Rose, use a disclaimer such as this: “The postings on this site are my own and don't necessarily represent those of Tudor Rose”.

6.9.9 Do link back to the source – when you do make a reference to a client, business partner or supplier, where possible link back to the source.

6.9.10 Be aware of your association with Tudor Rose internet and social media – If you identify yourself as a Tudor Rose employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and customers.

6.9.11 Remember that there are always consequences to what you publish. If you're about to publish something that makes you even the slightest bit uncomfortable, review the suggestions above and think about why that is. If you’re still unsure, and it is related to Tudor Rose business, feel free to discuss it with your line manager or simply do not publish it. You have sole responsibility for what you post to your blog or publish in any form of social media.

6.9.12 Do not use offensive content, personal insults, obscenity, or engage in any conduct that would not be acceptable in the Tudor Rose workplace. You should also show proper consideration for others’ privacy and for topics that may be considered objectionable or inflammatory.

6.9.13 Do not conduct confidential business with a customer or partner business through your personal or other internet or social media.

6.9.14 Do not register accounts using the Tudor Rose brand name or any other unregistered or registered trademarks.

6.9.15 Upon leaving Tudor Rose, employees are required to change their status on media websites such as LinkedIn to reflect their change in employment so as to not imply or state they remain in employment with Tudor Rose

6.10 E-mail, internet and social media is commonly used by the online criminal community to deliver malware and carry out schemes designed to damage property or steal confidential information. To minimize risk related to such threats, adhere to the following guidelines. While these guidelines help to reduce risk, they do not cover all possible threats and are not a substitute for good judgment.

6.10.1 Do not use the same passwords for social media that you use to access company computing resources.

6.10.2 Do not follow links on posted by individuals or organizations that you do not know.

6.10.3 Do not download software posted or recommended by individuals or organizations that you do not know.

6.10.4 If any content you find on any social media or web page looks suspicious in any way, close your browser and do not return to that page.

6.10.5 Configure social media accounts to encrypt communications whenever possible. Facebook, Twitter and others support encryption as an option. This is extremely important for roaming users who connect via public wi-fi networks.

6.10.6 Tudor Rose may employ technical controls to provide reminders, monitor, and enforce these guidelines.

**7. Instant and Video Messaging**

7.1 Instant messaging and video messaging is not currently supported by Tudor Rose.

7.2 Do not install or use Skype, Lync or any other instant or video messaging service on your Tudor Rose devices and do not use web-based instant messaging services such as those integrated with Facebook.

7.3 If you have a business critical reason to use instant or video messaging, consult your line manager and the ICT Manager before proceeding.

**8. Working remotely**

8.1 All electronic remote working must only be carried out on Tudor Rose equipment or services supplied by Tudor Rose. Sending documents to a home email account and working on your own device is prohibited unless you have obtained advance permission from your line manager and the ICT Manager.

8.2 When working remotely you must:

8.2.1 When in a public place never leave ICT devices unattended.

8.2.2 Password protect any work which relates to Tudor Rose's business so that no other person can access your work.

8.2.3 Position yourself so that your work cannot be overlooked by any other person.

8.2.4 Take reasonable precautions to safeguard the security of our laptop computers and any computer equipment on which you do Tudor Rose's business, and keep your passwords secret.

8.2.5 Inform the IT Manager within 24 hours if either a Tudor Rose device in your possession or any computer equipment on which you do Tudor Rose work has been lost or stolen.

8.2.6 Ensure that any work which you do remotely is saved on Tudor Rose's network or is transferred to the network as soon as reasonably practicable.

8.3 Tudor Rose has a zero-tolerance policy using devices while driving. Only hands-free talking while driving is permitted and then only when safe and legal to do so.

**9. Personal Use of ICT**

9.1 We do not prohibit personal use of ICT supplied by Tudor Rose, but we require you to use within reason and without negative impact on your responsibilities and performance.

9.2 Personal use – including but not limited to personal telephone calls, browsing the internet, e-mailing friends and family, using social media and addressing personal matters such as bills and shopping – must not incur any cost to the company and must not interrupt the work of your colleagues.

9.3 All personal emails and documents must be stored in files marked 'Personal'.

9.4 Personal use must not contravene the ICT Policy.

9.5 The following scenarios would be typically considered as unacceptable personal use of ICT:

9.5.1 Making personal long-distance telephone calls.

9.5.2 Using a work email address to apply for new jobs.

9.5.3 Forwarding a joke received by email onto colleagues and external recipients.

9.5.4 Subscribing to internet forums using a work email address.

9.5.5 Replying to multiple emails throughout the day to organising non-work related social activities.

9.5.6 Having personal social media alerts activated throughout working hours.

9.5.7 Making personal calls to premium rate telephone numbers.

9.6 All staff are reminded to ensure that they comply with GDPR and the principles of misusing data kept about living identifiable persons. If unsure about any Data Protection issue staff should contact Tudor Rose's nominated Data Protection Officer, Jon Ingleton.

**11. Personal Devices**

11.1 You may use your own devices to access Tudor Rose ICT which is hosted by a third party, which includes email, calendars, contacts, and web-based applications including CRM.

11.2 Any devices used to access ICT listed in 11.1 should be adequately password-protected in order that they cannot be accessed by others if lost or stolen.

11.3 Do not use your own devices to access the corporate network in any way. For example, do not plug your personal mobile phone into your work laptop.

11.4 Personal devices must not be used in any way that contravenes the ICT Policy.

11.5 Do not connect personal storage devices including memory sticks to Tudor Rose ICT without the express prior permission of your line manager and the ICT Manager, and not for any purpose that would contravene the ICT Policy.

**12. Acknowledgement**

Please complete the below and return this page only to the Human Resources Manager.

I agree that I have received, read and understand the Tudor Rose Information and Communications Technology Policy, dated May 2018.

Employee signature ……

Employee name ……

Date ……