*If you have adopted an IT, communications and monitoring policy, include the following:*

**Computer, Internet and Phone Usage Policy**

**Aims:**

* Understand how the internet, computers, emails and phones are to be used
* Understand the company policy governing their use

[Company name] provides employees with access to various computer and phone facilities for work and communication purposes. In order to ensure compliance with all applicable laws in relation to data protection, information security and compliance monitoring, the Company has adopted this policy which explains our approach to the use of computers, telephones and other devices by those who work for or with us.

This policy applies to all [name of business]’s employees and anyone else working for [name of business], including consultants, contractors, volunteers, interns, casual and agency workers.

This policy is not part of your employment contract and the company reserves the right to amend this policy at any time.

Breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Company’s formal discipline procedure.

Employees who consider that there has been a breach of this policy in relation to personal information about them held by the Company should raise the matter via the Company’s formal Grievance Procedure.

**IT, communications and monitoring**

The company makes extensive use of IT systems, for data storage, communications and as a source of information. We have adopted an IT, communications and monitoring policy in order to:-

* prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material);
* protect confidential, personal or commercially sensitive data;
* prevent the introduction of viruses;
* prevent the use of unlicensed software;
* ensure that company property is properly looked after;
* monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse.

**IT, communication and monitoring policy**

[Company name] (“the Company”) provides you with access to various computing, telephone and postage facilities (“the Facilities”) to allow you to undertake the responsibilities of your position and to improve internal and external communication.

This Policy sets out the Company’s policy on your use of the Facilities and it includes:-

* your responsibilities and potential liability when using the Facilities
* the monitoring policies adopted by the Company; and
* guidance on how to use the Facilities.

This Policy has been created to:-

* ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring
* protect the Company and its employees from the risk of financial loss, loss of reputation or libel; and
* ensure that the Facilities are not used so as to cause harm or damage to any person or organisation.

This Policy applies to the use of:-

* local, inter-office, national and international, private or public networks (including the Internet and Intranet) and all systems and services accessed through those networks
* desktop, portable and mobile computers and applications (including personal digital assistants (PDAs)
* mobile telephones (including the use of WAP services); and
* electronic mail and messaging services.

**Use of computer systems**

Subject to anything to the contrary in this Policy computers must be used for business purposes only.

In order to maintain the confidentiality of information held on or transferred via the Company’s computers, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Company’s network. Despite your use of a password, the Company reserves the right to override your password and obtain access to any part of the Facilities.

You are responsible for keeping your password secure. You must not give it to anyone, including colleagues, except as expressly authorised by the Company.

You are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Company or its clients other than in the normal and proper course of carrying out your duties for the Company.

In order to ensure proper use of computers, you must adhere to the following practices:-

* anti-virus software must be kept running at all times
* all forms of media storage must be checked by the [IT Department] before the contents are accessed or stored on the Company’s network or hard drives
* obvious passwords such as birthdays and spouse names etc must be avoided. The most secure passwords are random combinations of letters and numbers
* when you are sending data or software to an external party by floppy disk always ensure that the disk has been checked for viruses by the [IT Department] before sending it
* all files must be stored on the network drive which is backed up regularly to avoid loss of information; and
* always log off the network before leaving your computer for long periods of time or overnight.

**Software**

Software piracy could expose both the Company and the user to allegations of intellectual property infringement. The Company are committed to following the terms of all software licences to which the Company is a contracting party.

This means, in particular, that:

* software must not be installed onto any of the Company’s computers unless this has been approved in advance by the [IT Department]. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities
* software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of the [IT Department].

**Laptop Computers**

At various times during your employment with the Company, you may use a laptop. These computers, along with related equipment and software, are subject to all of the Company’s policies and guidelines governing non-portable computers and software (see two paragraphs in software section above). However, use of a laptop creates additional problems especially in respect of potential breaches of confidentiality.

When using a laptop:-

* you are responsible for all equipment and software until you return it. The laptop must be kept secure at all times
* you are the only person authorised to use the equipment and software issued to you
* you must not load or install files from any sources without the [IT Department] inspecting such files for viruses
* all data kept on the laptop must be backed up regularly in order to protect data against theft or mechanical failure or corruption
* you must password protect confidential data on disks or on the hard drive to protect against theft
* if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of the [IT Department]
* upon the request of the Company at any time, for any reason, you will immediately return any laptop, equipment and all software to the Company; and
* if you are using your own laptop to connect with the Company’s network or to transfer data between the laptop and any of the Company’s computers you must ensure that you have obtained prior consent of the [IT Department], comply with its instructions and ensure that any data downloaded or uploaded is free from viruses.

**Portable storage devices, (like USB sticks and portable hard drives)**

The company does not permit you to use portable storage devices (e.g. USB sticks and portable hard drives) without express authorisation. This is because their size and storage capacity make them vulnerable to misuse and to being mislaid. So, we do not favour their usage in our business and you may only use one of these devices to transfer data to a third-party computer (including your home computer) with prior consent to a specific transfer from specify person. You will commit gross misconduct if you breach this paragraph by transferring name of your business confidential data to a competitor

**Use of E-mail (Internal Or External Use)**

As a [name of your business] employee, you’ll have an email address, access to internal and external emails and the use of the internet. We provide these to you exclusively for the use in performing your contractual duties to our business.

We take all reasonable steps to protect our legal interests and the permissions and arrangements that we put in place relating to email and internet usage by you are no exception. This is because, for example, a carelessly worded or inadvertent ‘reply all’ email can cause significant damage to our trading relationships, deal prospects and/or reputation. It might cause a contract to be formed where we would not have intended it to be formed (or not on such terms). It may even give rise to a legal action against us, and potentially you also.

For these and other reasons, we have therefore adopted the email, communications services and internet use policy set out below and all company employees are expected to comply with it or risk disciplinary action.

Internet e-mail is not a secure medium of communication – it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by e-mail this should be sent using password protected attachments.

E-mail should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the e-mail.

Do not forward e-mail messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the e-mail.

You should not use email to send unsolicited correspondence or email marketing campaigns. This is especially important in light of the company’s obligations under Ireland’s data protection legislation and the rules relating to recipient consent to the receipt of unsolicited correspondence.

Your e-mail inbox should be checked on a regular basis.

If you are away from the office and use e-mail as an external means of communication, you must ensure that the autoreply service is used to inform the sender that you are unavailable. Failure to do so could lead to disciplinary action. If you have any doubt as to how to use these facilities, please contact the [IT Department].

Email should generally not be used for private and personal purposes, during or after working hours. You should not use the company’s email to circulate any non-business content, including photos.

The company takes these rules very seriously. In particular, name of your business will not tolerate any use of our internet or email facilities that results in the bullying, harassment or intimidation of any of our employees and any offensive remarks, pictures or jokes may be considered unlawful harassment necessitating disciplinary action by us, potentially for gross misconduct, which may result in your dismissal.

**Use of the Internet**

Use of the Internet, or Internet services, by unauthorised users is strictly prohibited. You are responsible for ensuring that you are the only person using your authorised Internet account and services.

Downloads of material and information from the internet should only be made by you on to our equipment where the download:

1. is required to enable you to fulfil your duties to the business, and
2. has been authorised by specify person, who has confirmed that this appears to be a permitted activity and would not appear to infringe any third-party intellectual property.

Viewing, downloading, storing (including data held in RAM or cache) displaying or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Posting information on the Internet, whether on a newsgroup, via a chat room or via e-mail is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting and the Company could face legal claims for monetary damages.

{Using the Internet for the purpose of trading or carrying out any business activity other than Company business is strictly prohibited.}

**OR**

[Subject to the above you are allowed to use the Internet for personal use during your lunch break. Use of the Internet for personal use at any other time is strictly prohibited.]

Unacceptable internet activities include, for example:

1. unauthorised downloading and/or file-sharing of any material (e.g. films or music) that is protected by copyright and therefore infringes that copyright
2. visiting gambling or sexually explicit/pornographic sites
3. downloading or circulating in any manner or format, grossly offensive, obscene or illegal material, or
4. otherwise using the internet for illegal activities.

Engaging in any such activity will be treated as gross misconduct by name of your business and you are likely to face dismissal under our disciplinary process.

**Social media**

We may permit employees to use our internet facilities to engage in social networking and video-sharing services such as Facebook, Twitter, LinkedIn, YouTube, provided that these are not permitted to be a distraction to their contractual duties and they are only engaged with during breaks and out of working hours.

You should also ensure that you comply with the terms of our separate Social Media Policy. A copy of this policy is available specify location/person.

**Monitoring of your email and internet usage**

Your email communications are not private.

Where we consider it necessary and appropriate, we may monitor your internet and email usage. We may do this as part of a routine systems and security audit, to help manage your absence from the business (e.g. where you are on sick leave and communications need to be checked and/or answered in your absence), or where a concern has arisen about excessive or inappropriate use by you of our internet and/or email systems.

In most cases, name of your business will confine itself to monitoring addresses and headings of emails. But it is not prevented from opening emails and viewing the actual contents and it may do so in exceptional cases.

You should not use our email systems to send any communications that contain highly sensitive and confidential contents. Where you do send occasional personal emails, they should ideally be marked as ‘personal’ and name of your business will, where possible, aim to avoid opening such emails unless it has good reason to do so.

The Company will not (unless required by law):-

* allow third parties to monitor your email and internet use; or
* disclose information obtained by such monitoring to third parties.

The Company may be prohibited by law from notifying employees of a disclosure to third parties.

**Use of Telephones**

The company’s telephone systems and equipment exist to further the business activities and interests of the company. As one of our employees, you are permitted to use our equipment and systems in order to carry out the role for which we appointed you.

**Misuse of telephone equipment or systems**

Our telephone equipment and systems are only for use by our workers in connection with our business.

Employees are permitted to make occasional personal calls using our telephone system, provided that these calls are limited in both call duration and occurrence. In all but exceptional circumstances, such calls should be made or taken during breaks, so as to cause minimum disruption to the employee’s productivity and that of others with whom the employee may be working at the time of the call.

Excessive and unreasonable use of our telephones for personal calls will not be permitted and will be handled as a disciplinary matter under our Disciplinary Policy and Procedures and you will be required to reimburse name of your business for the costs that we have incurred. (‘Unreasonable use’ includes making calls at premium rates and/or abroad.)

**Monitoring of calls and voicemails and maintenance of call logs by name of your business**

Calls made and received on our telephone network may be routinely monitored and recorded so that, for example, name of your business can assess employee performance, the appropriateness of employee behaviour, and/or levels of customer satisfaction. We may keep an itemised call log of calls made and received on our telephone network and this can include details of the caller’s number, date of the call, time and duration of the call and to whom within our business it was made. It is possible that personal calls may be heard, recorded and logged as a result, although name of your business will generally not retain any recordings of personal calls, save in exceptional circumstances where their content relates to a matter concerning your conduct that is under investigation by name of your business.

Voicemails may be similarly recorded and itemised. They may be accessed and listened to by someone designated by name of your business where the recipient is absent and unable to take receipt of the message, which could be important or urgent. Personal messages might well be heard as part of this exercise.

**Use of mobile phones**

The company accepts that employees will want to use their own mobile phones for essential personal calls during normal working hours, and this is acceptable, though we encourage all employees to keep calls to a minimum and to be considerate towards others in both the volume of their ringtones (ideally, phones should be set to silent) and the frequency of those calls.

Excessive making or taking of personal calls on your mobile phone is not acceptable and will be handled as a disciplinary matter, as will use of a personal mobile phone for excessive periods and/or at inappropriate times or for inappropriate purposes, to browse the internet, engage in personal social media activity, text message (in any format, including by use of an instant messaging app), take videos, make sound recordings or take pictures.

This section is however, most principally concerned with the provision of a [name of your business] business mobile phone to you, and the manner in which you may use it to fulfil your contractual duties to us as our employee.

**Provision of mobile devices by name of your business**

If the company provides you with a mobile phone, you must use it exclusively for our business purposes during working hours.

You may take or make occasional calls on this mobile phone for personal reasons. However, the excessive and/or unreasonable making or taking of personal calls on this mobile phone is not acceptable and will be handled as a disciplinary offence. ‘Unreasonable usage’ includes personal calls to premium rate lines and international calls.

The excessive use of this mobile phone to browse the internet for personal reasons, and any engagement in personal social media activity and personal text messaging (in any format, including by use of an instant messaging app), the making of videos, sound recordings or taking of pictures for personal reasons, is also not allowed and will equally be treated as a disciplinary matter.

Each month, the company receives an itemised list of all calls and texts made on the mobile phone, as well as details of data usage, from our service provider. The list discloses the number and length of calls, the number of texts, the costs of each and the numbers dialled or texted by you.

The company has the right to install mobile device management software on to any relevant device that it provides to you. This software enables us to:

1. remotely wipe the content of the phone, which may be necessary in the event of it being lost or stolen, and
2. set passwords, pins and reset security features.

**Costs of personal calls on [name of business]’s mobile devices**

We will pay, on a monthly basis, the network rental costs for the mobile phone, which will generally include an allowance on minutes for calls made, texts sent and data used.

If you exceed any of these allowances, we will require you to pay the costs incurred, where these costs have not been generated by your use of the mobile phone for our business purposes. Where your allowance has been exceeded, we will ask you to identify which usage is for genuine business purposes and which items are attributable to personal usage.

You agree to consent to the company deducting the cost of any personal usage that exceeds your monthly allowance from your salary and your signature at the end of this policy confirms this agreement.

**Loss or theft of the phone**

If, because of your negligence or carelessness, you lose the phone and/or its accessories, (including any cases and chargers that we provide to you), or it is/they are stolen, you will be required to reimburse us for the cost of a like-for-like phone and/or accessories replacement (or as close to that position as we can reasonably get). Your signature at the end of this policy confirms your agreement to reimbursing us in these circumstances.

We have the right to request the return of the phone and any accessories at any point during your employment with [name of your business].

**Return of the phone on conclusion of your contract**

You must return the phone and any accessories to us by the end of business hours on the final day of your employment with us (whatever the reason for its termination). If you fail to do so, we will be entitled to withhold the equivalent value of the phone and any accessories from your wages until they are returned to us; and if they are not returned to us within 24 hours after the expiry of your final day of employment, we may permanently deduct the cost and retain those withheld wages. Your signature at the end of this policy confirms that you understand and agree to this.

**What happens where [name of your business] authorises you to use your own devices to carry out your contractual duties**

If the company expressly authorises you to use your own mobile phone for business purposes and then claim back the related costs, the following rules will apply.

During working hours, you must use your mobile phone exclusively for our business purposes. However, exceptionally, during working hours, you may take or make occasional calls on your mobile phone for personal reasons. The excessive and/or unreasonable making or taking of personal calls on your mobile phone is not acceptable and will be handled as a disciplinary offence (whether or not you attempt to claim back the related expenses from us). ‘Unreasonable usage’ includes personal calls to premium rate lines and international calls, unless such usage has been expressly authorised in advance by name of your business.

During working hours, the excessive use of your mobile phone to browse the internet for personal reasons, and any engagement in personal social media activity and personal text messaging (in any format, including by use of an instant messaging app), the making of videos, sound recordings or taking of pictures for personal reasons, is also not allowed and will equally be treated as a disciplinary matter.

You should reclaim any expenses related to the use of your mobile phone for [name of your business]’s business purposes in accordance with our [name expenses policy], details of which can be found [insert details] **OR** our usual approach to expenses claims, please ask [specify person] for more details if you need these. Any attempt to reclaim expenses related to your personal use of your mobile phone is prohibited and will be handled as a serious disciplinary offence.

**Driving while using a mobile phone**

Never use a hand-held mobile phone while driving or operating machinery. Using a hand-held mobile phone when you are driving a vehicle is a criminal offence. This applies whether you are making or receiving calls, texts or emails, listening to voicemails or viewing images, for example. For whatever you may use a phone, handling it is prohibited in these circumstances.

Whether you use a [name of your business] mobile phone, or we have given you permission to use your own phone for our business purposes, if you are discovered contravening this rule you may face serious disciplinary action under our disciplinary policy and procedures.

If you need to drive as part of your business duties for [name of your business], you may use a genuinely hands-free mobile phone while you are driving. By ‘hands-free’, we mean that at no point in its operation do you need to hold or touch the mobile phone. For example, a hands-free mobile phone that is voice-activated or one that is positioned in a cradle and can be connected to car speakers and activated from the steering wheel would be considered genuinely hands-free. We strongly recommend, however, that even this hands-free phone activity is in any event restricted to what is strictly necessary and that as far as possible, calls that you do receive or make are kept short, to minimise distractions while you are driving, which is in the interests of your general road safety.

I have read and accept the terms of this policy. I agree to [name of your business] making deductions from my salary where these deductions prove necessary according to this policy.

Signed: