General Computer, Email, Intranet, Internet Acceptable Usage Policy

General Comments -

* This is a template/precedent document only. It should be tailored as appropriate to suit the needs of each individual firm.
* All sections should be considered and implemented as deemed appropriate for the firm. This cover page should not be included.
* The LQSI cannot accept any responsibility for any errors or omissions contained in this template document.
* The document should be reviewed on an annual basis, or as required.

Specific Comments -

* This policy was generally reviewed in February 2021.
* The policy has been amended to reflect the requirement for firms to have control procedures in place in relation to the use of USB devices.

The Legal Quality Standard of Ireland

Reviewed February 2023

General Computer, Email, Intranet, Internet Acceptable Usage Policy

This document sets out the Firm’s policy for general computer, email, intranet and internet usage. It seeks to provide advice and assistance to you in your use of email, the intranet and the internet at work and also lists the rules about Computer, Email, Intranet and Internet usage that you must follow.

These rules have been designed to ensure that the firm and you get the most from computer systems including email, (the intranet) and the internet without imposing an unnecessary cost burden on the Firm. The Firm regards any breach of this policy as a serious matter. Any failure or refusal to comply with this policy is a disciplinary offence which may lead to disciplinary action, up to and including, dismissal without notice. You need to be aware that breach of the policy can lead to criminal liabilities for the Firm.

I acknowledge receipt of XXXX, Solicitors’ GCEIIUP and I agree to be bound by the rules contained in that document.

User Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Block Capitals)

Department: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Block Capitals)

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Managers Authorisation:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Block Capitals)

Position: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

General Computer Usage Policy

This policy applies to all [firm name] Solicitors computer users including those without access to Email, the Intranet or the Internet.

1. User Ids and Passwords

User Ids and passwords help maintain individual accountability for computer resource usage. Any employee who obtains a password for accessing the Firm’s Computer resource must keep that password confidential. Firm policy prohibits the sharing of user Ids and passwords for all computer systems including those used for access to business applications, Email, Intranet, Internet etc. However, the Firm’s IT Provider may from time to time need to reset a user’s password in order to carry out support tasks. IT personnel will inform the user and supply the temporary password; it is the user’s responsibility to ensure that their temporarily assigned password is changed after such an instance. Passwords should not be written down. (See Password policy for further information)

1. Use of Company Computing Facilities

Employees may not use the Firm’s facilities in a manner that would disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

<<Firm Name>>, Solicitors computers are installed and maintained for the Firm’s business purposes and are not for personal use.

1. Installation and Downloading of Software

Software in use on XXXX, Solicitors computers is licensed and must not be reproduced or copied in any format.

The installing and/or downloading of computer software onto the Firm computers is the exclusive responsibility of XXXX, Solicitors IT staff/External IT Providers. Furthermore, non-IT staff are not permitted to alter settings on XXXX, Solicitors computers.

1. Installing of Computer Hardware and Computer Peripherals

The installing of computer hardware and computer peripherals on to the Firm networks/computers is the exclusive responsibility of the Firm’s IT personnel or personnel designated by the Firm’s IT staff/External IT Providers.

1. Externally provided USB devices or other Media

The firm prohibits the use of USB devices or other media.  *OR* The introduction of memory sticks, USB Devices or other media onto XXXX, Solicitors computers can only be done with the prior knowledge and approval of XXXX, Solicitors IT Staff/External IT Providers.

1. Legal Usage

Computer resources and network capacity may not be used for illegal purposes. Examples of illegal purpose include but are not limited to:

* Harassment of other users
* Destruction of or damage to equipment, software, or data belonging to the Firm
* Disruption or unauthorized monitoring of electronic communications
* Violations of computer system security
* Unauthorized use of computer accounts, access codes, etc
* Installation/download of offensive, pornographic or racist material

1. The rights of XXXX, Solicitors to inspect computer files / records.

The Firm reserves the right to inspect any and all files stored on its network, servers, PCs etc. in order to ensure compliance with this policy.

1. Disable access to unattended PCs terminals

All personnel when leaving their PC/ Terminal unattended must ensure the PC/Terminal is locked to prevent unauthorised access.

1. Remote Access to the Firms Network

* Remote access to the Firm’s network from an employee’s laptop/smart phone or tablet is only allotted to designated employees by the firms IT Staff or External IT Providers.
* All confidential and restricted information transmitted via a remote access connection must be encrypted prior to transmission or sent through an encrypted tunnel.
* Remote access connections must only be used for approved legal purposes.
* All computer devices that are connected to the Firm’s network remotely must have up to date anti-virus software installed on their mobile device.
* All remote access sessions which are inactive for more than 30 minutes must be automatically ‘locked’ or logged out. Where this is not possible, users must be instructed to manually log off or ‘lock’ their computer device when they have to leave it unattended for any period of time.
* Employees should also consult the firm’s Agile and Remote Working Policy and any other related IT Security and GDPR policies.

Email Usage Policy

Introduction

This email policy covers all email usage including laptops, tablets, personal handheld devices such as smart phones, iPhones etc. Email is a personal computerised and efficient communication system that enables the sending and receiving of messages between the Firm’s staff and its clients and business partners. External email is sent / received via the Internet some of the Firm’s Internet Usage policies also apply to email. This email policy covers the email itself and any documents or other material that are attached to emails.

There are some risks attached to the sending of emails as set out below:

* Remember that email is effectively on official headed paper and can be traced back to place, date and time of sending. Make sure you are satisfied with its content and that it has been approved at the appropriate level. Double check the address of the intended recipient. Once the ‘send’ key is pressed, email cannot be stopped or retrieved. Deleting an email from your system does not make it untraceable.
* Email is a form of publishing. Thus, libel and defamation laws apply that would not count in private conversations or correspondence.
* Your message may go to the persons or be intercepted by persons other than the intended recipient and, if confidential or commercially sensitive, this could be damaging to the Firm.
* Letters, files and other documents attached to emails may belong to others and there may be copyright implications in sending or receiving them without permission.
* Email messages may legally bind the firm contractually in certain instances without the proper authority being obtained internally.
* Email communications are not always assumed privileged communications. Communications which qualify as privileged communications are those which contain legal advice. Not all email communications can be assumed to contain legal advice.
* All personal data contained in emails may be accessible under the General Data Protection Regulation and the Data Protection Act 2018 and furthermore, a substantial portion of emails to Government and other public bodies may be accessible under Freedom of Information legislation.
* Email is speedy and as such messages written in haste or written carelessly would give rise to legal liability on the firms part such as claims for defamation etc.
* Email messages to a particular address may be intercepted, viewed by other persons in the addressee organisation, forwarded without your knowledge, altered or cut and pasted into another email without authority*.* If client communications are conducted via email, any legal advices, Section 150 notice/engagement letter and acceptance of instructions or changes in instructions must be sent in the form of a covering letter with the firm’s letterhead to the client in PDF format only. This ensures that any of the content will not be interfered or tampered with in any way.
* Instructions or changes in instructions by the client via email will not be deemed to be accepted by the firm unless a confirmatory email, telephone call with an attendance placed on the file or a letter is sent back by the fee earner to the client.
* Email messages can carry computer viruses which are damaging to the firm’s / others computer systems.

The above risks are taken into account in formulating the following Email Acceptable usage policy.

Rules of Acceptable Usage

1. Email messages must be appropriate and professional. The firm’s name which is included in every message reflects on the firm’s image and reputation.
2. The firm email system is installed and maintained primarily for business purposes. You may send some personal messages, but such messages should be minimised and kept as short as possible. Personal emails are also governed by the Acceptable Use Rules as set out in this policy.
3. Confidential or commercially sensitive information should not be sent by email unless you are using appropriate encryption procedures.
4. Employees may not send chain letters, any form of mass mailing or engage in spamming.
5. Extra caution must be taken with email messages in respect of disparaging remarks contained therein. Do not use indecent, obscene, sexist, racist or other inappropriate remarks in written form, in cartoon form, or otherwise.
6. If you receive any offensive, unpleasant, harassing or intimidating messages via email you are requested to inform the office manager or firms IT Provider immediately. It is important that such messages are traced as quickly as possible.
7. Documents or other material that would breach copyright must not be attached to emails.
8. Email users must not access the email of colleagues without the colleagues’ and/or management’s permission.
9. The firm-approved disclaimer must be attached to all emails.
10. The firm has content filtering software in place that may be used to intercept unsuitable material either entering or leaving the firm through the email system.
11. All business-related email must be sent by the secure firm’s email system provided on user PCs e.g. Google Mail or MS Outlook. Whilst access to Internet-based or other mail systems e.g. Hotmail, Gmail, etc is acceptable this should be restricted to out of office hours i.e. pre-9.00am, between 1.00pm and 2.00pm and after 5.30pm except in exceptional circumstances.
12. Information that contains personal data (that relates to an individual which includes sole trade businesses) must be dealt with in accordance with the firm’s Data Protection Policy
13. The firmreserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose. All computer pass codes must be provided to *(office manager/managing partner/ External IT Providers).* No pass code may be used that is unknown to the firm.
14. Notwithstanding the firms right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them.
15. Any exception to this policy must receive prior approval from the firm. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message. If any breach of our E-mail policy is observed then disciplinary action up to and including dismissal may be taken.

Intranet Usage Policy (relevant only in circumstances where a firm has an intranet – delete if not applicable)

Introduction

The Intranet is a powerful tool for sharing information within the firm. The information included on the intranet will include information which is important and confidential to the firm and, if this is used inappropriately, it could have serious consequences for the firm.

This intranet usage policy is designed to help you understand the firm expectation for use of the Intranet.

You are required to use the intranet in accordance with all existing the existing practice policies and to respect copyright, software licensing rules, property rights, privacy, data protection requirements, confidentiality, information and data security when using the intranet.

Rules of acceptable use

1. You should treat information which you obtain from the intranet as confidential information and only disclose it to people who are authorised to receive it.
2. Any information which you download from the intranet which contains personal data (information relating to an individual which includes sole trade businesses) must be dealt with in accordance with the firms Data Protection Policy.
3. Before adding any information to the intranet which contains personal data, make sure you have complied with the firms Data Protection Policy and remember that the individual is entitled to access such information.
4. The firm has software and systems in place that monitor and record all intranet usage. The chief reason for deploying these systems is to assure the safety and security of the firms network. Any employee who attempts to disable, defeat or circumvent any company security facility will be subject to disciplinary action that may lead to dismissal without notice.
5. User IDs and passwords help maintain individual accountability for intranet resource usage. Any employee who obtains a password or ID for an intranet resource must keep that password confidential. Firm policy prohibits the sharing of user IDs and passwords for all systems including those obtained for access to the intranet.
6. As set out in the email policy all contributions postings etc. will be subject to libel and defamation laws apply that would not count in private conversations or correspondence and you should not post or use any information that contains indecent, obscene, sexist, racist or other inappropriate remarks in written form, in cartoon form, or otherwise that would cause offence to or refers to any other employee of the firm.
7. The firm may withdraw or reduce your access to the intranet at any time.
8. The information in the intranet should not be relied upon for any purpose other than to allow you to perform your role within the firm. The Intranet may contain information which is provided to enable employees to perform their roles effectively within the firm (such as information about the performance of the firm, its clients and competitors) and this information should not be relied upon when not performing these roles (such as deciding whether to buy shares in any clients of the firm).
9. This intranet site contains material which is owned by or licensed to the firm. This material includes, but is not limited to, the design, layout, look, appearance and graphics. It is protected by intellectual property laws including, but not limited to, copyright.

Internet Usage Policy

Introduction

The Internet is a powerful tool for accessing information and communicating with external organisations and individuals. However, the internet suffers from significant and widespread security and integrity risks and has the potential to be used in ways that are inappropriate to the goals of the firm.

The facilities to provide internet access represent a considerable commitment of company resources for telecommunications, networking, software, storage, etc. This internet usage policy is designed to help you understand the firms expectations for the use of this resource. As the internet is a business tool, provided to you at significant cost, you are expected during office hours to use your internet access for business-related purposes. You are required to conduct yourself appropriately on the internet (i.e. all existing company policies apply) and to respect copyright, software licensing rules, property rights, privacy, confidentiality, information and data security, etc. at all times when using the firms resources to access the Internet.

The following Internet Acceptable Usage Policy covers administration, technical and security considerations.

Rules of Acceptable Usage

1. The firm has software and systems in place that monitor and record all Internet usage. The chief reason for deploying these systems is to assure the safety and security of the firms network. Any employee who attempts to disable, defeat or circumvent any company security facility will be subject to disciplinary action that may lead to dismissal.
2. Any files or software downloaded via the internet onto the firms network become the property of the firm. Any such files or software may be used only in ways that are consistent with their licences or copyright. Software is not to be downloaded without prior approval of the Office Manager/External IT Provider.
3. The firm reserves the right to inspect any and all files stored on its network/on its PCs in order to ensure compliance with policy.
4. User IDs and passwords help maintain individual accountability for internet resource usage. Any employee who obtains a password or ID for an internet resource must keep that password confidential. Company policy prohibits the sharing of user IDs and passwords for all systems including those obtained for access to internet sites. Please review the requirements of the firm’s password policy.
5. Sexually explicit, pornographic, racist, profane or other offensive material may not be accessed, downloaded, displayed, archived, stored, distributed or recorded using the firm network or computing resources.
6. Employees may not use the firms internet facilities to download or distribute pirated material (software or data) or to download images, video or audio unless in the case of the latter downloads there is a business-related use for the material.
7. Employees may not use the firms internet facilities to deliberately propagate any virus, worm, or Trojan horse code.
8. Employees may not use the firms facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
9. The use of social networking sites such as but not limited to Facebook, Instagram, Twitter etc newsgroup and chat room forums are forbidden except for authorised personnel and even then, only for specific business purposes. Please refer to the firms Social Media Policy.
10. All email must be sent by the secure firms email system provided on user PCs. Whilst access to Internet-based or other email systems e.g. Hotmail, gmail, is acceptable this should be restricted to outside office hours i.e. pre-9.00am, between 1.00pm and 2.00pm and after 5.30pm except in exceptional circumstances.

Any breaches of these rules will be treated seriously and will be subject to disciplinary action up to and including dismissal. For details of our disciplinary procedures please refer to the firms Employee Handbook.

Signed:

Dated:

Date of next review: