
# THE LAW SOCIETY OF IRELAND

# IT SECURITY POLICY

| | |
|---|---|
| **Version Number:** | 1 |
| **Date:** | 24 May 2018 |

## CONTENTS

**Section** **Page**

# Law Society of Ireland IT Security Policy

## Introduction

The Law Society has very strict guidelines on the use and abuse of its e-mail, Internet, telephone, voicemail and ICT systems in general**. You are required to familiarise yourself with and adhere to these policies and procedures**. This document provides specific instructions on all aspects of the usage of these systems, and if you are in any doubt, please contacts the IT Manager for clarification.

The reader should use this document as a general introduction to the topic of Information Technology Security and Usage, and to the approach taken by the Society to ensure all our information assets are safe and secure. This policy applies to all information systems (System 360 (Aptify), Sun Accounts, Membership and Education Databases, Library catalogue, PC's etc.) regardless of the Department they are in or the technology that is used. Standards, procedures and guidelines exist to support the implementation of this policy. These documents formalise the steps required to minimise the probability of a security incident compromising our information assets or impacting our ability to carry out our business. They identify the expected behaviour and responsibilities for every person using the Society's information systems.

## Purpose

- To provide a secure and productive computing environment for the Society.
- To increase awareness of computer security amongst staff and students of the Society.
- To increase the awareness of their responsibilities when using Society resources.
- To provide a guideline for protecting valuable information resources from theft, damage, and unauthorised access or change.
- To increase the awareness of confidentiality and possible legal requirements when dealing with sensitive Society information.

## The Society's Expectation of Users

- Users must use user-id for the specified Society's purposes, and must not use any other user's id with or without that user's permission.
- Users must protect their user-id and passwords from unauthorised use. Users are responsible for all activities, legal or otherwise, associated with their user-id.
- Electronic communications facilities (such as e-mail) should not be used to send fraudulent, harassing, obscene, threatening, or other unlawful messages. e-mail should not be used for the transmission of jokes.
- Users may not create, send or forward multi-level marketing letters (chain letters, pyramid selling schemes etc.)
- Users must not attempt to modify or remove computer equipment, software, or peripherals without proper authorisation.
- Users must familiarise themselves with best practice in relation to cyber security

non-adherence to these conditions may, after due process, result in any of the following:

- The suspension of computing privileges
- Disciplinary action in line with the Society's disciplinary procedures.

**Monitoring tools are in place for e-mail and Internet usage, logs of all mail through our gate-way and sites visited on the Internet are retained on the respective servers.**

**User-id's and Passwords**

Each user must change their password at least **every 45 days**. If you do not change your password within this period, the system will prompt you to do so. The password should be a minimum of 10 characters long (alpha and numerical with upper and lowercase letters)

The maximum number of failed login attempts is four, after which the access is automatically revoked. When requesting a reset, you should state if you had not had failed attempts. This way, the IT Section can see if there was attempted unauthorised access with your user-id and investigate accordingly. Password resets will be carried out as soon as possible, depending on the resources available in the IT Section. Thus, if the access is revoked, you may have to wait some time to get back network access.

**Guidelines for passwords**

- The password should not be related to the users name or user-id in any form
- Use a password that is easy to remember, that you don't have to write down.
- Use a password that can be typed quickly, without having to look at the keyboard
- Avoid using obvious passwords such as the name of a family member, car license plate, phone number, or any information that is easily obtained about you.
- Passwords of any sequentially incremental form should not be used (LawSociety1, LawSociety2, etc.)
- Passwords are not transferable among users. If a user needs access, it should be requested.
- The secrecy of a password is the responsibility of the user who will be held accountable for any and all use of that password.
- User-id & password = ATM card & PIN, and should be protected in the same way.

**Locking your computer and logging out**

You must always lock your PC when away from your desk.

You must always log out fully at the end of the day when you are finished your work. It is not sufficient to lock your computer or simply switch it off.

**Virus Protection**

In order to limit the spread of viruses, the Society has invested heavily in our anti-virus protection. Even though we have virus protection, there is always a risk of a new virus that we have not received an update for.

As we increasingly look to outside sources for information and e-mail, it is important we be aware of Virus Infection and the damage it can do. Introduction of viruses and other contaminants can occur through a variety of sources.

- A third party laptop being plugged onto our network, this should never be allowed. Request network access from IT instead.
- E-mail from any party, whether a trusted associate or a casual acquaintance. Do not launch, detach or save any executable file (i.e. those ending in 'exe' or 'vbs') under any circumstances
- USB Key's or CD's should be checked and scanned for viruses
- Software introduced into or used on the system by an outsider who has access to the sys- tem.
- Software used at home on an infected system
- Software purchased from a vendor who has an infected production system.
- Infected software from the Internet.

Anti-virus updates are sent automatically to all network PC's. Please note the following:

- Anti-Virus Software is installed on all Society PC's. This includes standalone PC's, Laptops, networked PC's and Servers
- Any virus alert or detection should be reported to the IT Section immediately where its occurrence will be logged, the source must be found and contacted, and the media dis- infected. **Do not use the PC any further until the IT Section has had a chance to investigate.**
- Loading of games and non-approved soft-ware onto PC's is strictly prohibited.
- All software loaded on the Society's PC's is fully licensed. **If the IT Section finds any unauthorised software, it will be removed immediately and may result in disciplinary action being taken.**

**E-mail usage policy**

The general address is: general@lawsociety.ie

The user-specific address takes the following format, e.g.: c.macdomhnaill@lawsociety.ie, m.kearney@lawsociety.ie

**In order to ensure that we get the best value from the E-mail system there are a number of standards that should be adhered to.**

Your e-mail account is for business use. E-mail is suitable for short communications, making arrangements and sending documents that can be printed off by the recipient.

A simple reminder, it is not what's to the left of the@ sign, it's what's to the right of the @ sign and, thus, anything you send can be misconstrued as the opinion of the Law Society rather than a careless mail from an individual. Think before you send. Think of e-mail as a postcard, written in pencil, and put in a post box. If you are happy to send something that anybody could alter, read, take, or may never be delivered, then put it in an e-mail.

Email should **not** be used:

- To send confidential information unless appropriately passworded or encrypted
- To try and discuss complex or lengthy issues. If necessary these should be put in a Word document which can be sent as an attachment. This is a speedy way of sending a letter but is the same as corresponding by letter or memo.
- To send chain letters/jokes etc. The issuing or forwarding of such mail items will be considered a disciplinary matter.

The Society strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, the Society prohibits the use of computers and the E-mail system in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-colour jokes, or anything that may be construed as harassment or showing disrespect for others. E-mail may not be used to solicit others for commercial ventures, religious or political causes, outside organisations, or other non-business matters.

The Society is bound by legislation such as the Child Trafficking and Pornography Act of 1998 for mandatory reporting of any persons or systems accessing inappropriate materials.

The Society employs two automated programmes.to stop all viruses, programs, images, profanities and other words that are associated with spam. If a genuine mail is stopped, it will be released on being discovered by a member of the IT Section, or at the request of the user. Due to the prevalence of viruses in e-mails, the IT Section will not be able to release any mail with an executable or virus attached.

**To ensure compliance with this policy, E-mail usage will be monitored. It is also recommended that your Law Society email account is not used as a Personal email account linked to, for example, utility bills or entertainment related accounts.**

### Internal E-mails

- It should focus on one subject per message and always include a pertinent subject title for the message; that way, the user can locate the message quickly.
- It should not be assumed that any messages are private or to be read by only yourself or the recipient. Never send something you would mind seeing on the evening news.
- When quoting another person, or forwarding on another E-mail, edit out whatever is not directly applicable to your reply.
- Capitalise words only rarely to highlight an important point or to distinguish a title or heading. Capitalising whole words that are not titles is GENERALLY VIEWED AS NEEDLESS SHOUTING.
- Be careful when using sarcasm and humour. Without face to face communications your joke may be seen as criticism.

However, note that if there is a possibility that the E-mail or its contents will be communicated externally then the standards below apply.

E-mail is a business tool and must be used as such and is not a medium for communication of jokes, rumours, gossip etc.

All E-mails referring to individuals may be released to those individuals under a data access request.

### External E-mails

External E-mails should be as formal and as professional as any external correspondence. Written internal correspondence may often be less formal than normal. This can also apply to internal E- mails. However, we must ensure that this does not spill over into external E-mails. Remember the quality of E-mails sent externally is as important as the quality of letters we dispatch. Each E-mail should:

- Start with the name of the person to whom it is addressed (do not assume that the recipient's E-mail address is sufficient). Use first name or first name and surname.
- Include your signature block at the bottom of the E-mail messages. Your signature footer should adhere to the Law Society standards include your name, position, company and e-mail address. This should not exceed more than 5 lines.
- Always finish with your own name or a clearly recognised abbreviation. Normal typing protocols should be used, e.g. capitals, paragraphs etc. For very short E-mails full sentences may be abbreviated

## Out of Office Assistant

It is the Society's policy to keep people advised of when we are out of the office for periods of time. We do this through voicemail and the Out of Office Assistant in Outlook. The Out of Office Assistant automatically replies to incoming messages while out of the office. It is easy to use.

In Outlook, click on File, Info then select Automatic Replies (Out of Office). Click on Send Automatic Replies. Click "Send Automatic replies", type the message you want to send to others while you are out.

It should state the period for which you are out, when you are due back in and who is handling your work in your absence.

Click on OK, and from that moment, the reply will go out for every mail that comes into your inbox.

NOTE: The Auto Reply is sent only once to each sender of an email during the period the out of office is set.

On returning to the office, go into Outlook, it will prompt you to turn off the Out of Office. It is important you do this so as everybody knows you're back in.

## Legal Position

It should be remembered that the contents of both internal and external E-mails are discoverable and may be used in legal proceedings. Consequently, the normal precautions that you would take in regard to "publishing" should be preserved. If you would not write it in a normal letter then definitely do not put it in an E-mail. Again, think of the analogy of the postcard, written in pencil, and put in a post box. If you are happy to send something that anybody could alter, read, take, or may never be delivered, then put it in an e-mail.

## Internet Usage Policy

Internet access enables staff to obtain information specific to their role within the Law Society of Ireland. Many of the Internet's activities are for recreational and private use and are unrelated to Law Society business. For that reason, full access to the Internet is restricted to staff members and certain PC's.

If you consider that you need Internet access to a specific site on your desktop, you should make application, giving the business case for Internet access, in writing to your Department head who will seek approval for access if appropriate.

Other staff members requiring access to the Internet can use the PC's in common areas. There are terminals in the Library, Vanilla Café Mezzanine and IT Room where the Internet can be accessed. If you need frequent access in the common areas, please contact the IT Administrator in the Education Centre for an ID. Otherwise, the library staff can log you into a terminal for your use.

The risk to the Law Society of Ireland from Internet usage are even greater than that with e-mail and hence the need for strict rules.

- The Law Society's Internet connections are intended for the activities that support either the Society's business or the professional development of employees. Staff members whom in the opinion of management have abused this will be subject to disciplinary action.
- Authorised personnel have the responsibility for Internet access under their password and hence will have responsibility for unauthorised use of that password with or without their consent.
- Information used, or presented, on the Internet should not violate the terms and conditions of copyright law or the terms of the Data Protection Acts/GDPR.
- The Internet should not be used for personal gain or profit, to post, download or circulate messages and materials that contain inappropriate, obscene, inflammatory, intimidatory, harassing, defamatory, disruptive, porno- graphic, sexist, racist or otherwise offensive language, materials, images or files.

The employee uses the Internet as an agent of the Law Society and must therefore maintain the highest degree of professionalism at all times. All communications with external organisations must constantly demonstrate this professionalism.

**All web browsing is logged. Screening software prevents access to certain non-work related sites. The logs of web browsing will only be accessed with management authorisation, where there are reasonable grounds to believe that this policy has been contravened.**

**The Society reserves the right to inspect a user's access to ensure compliance with Society policies and law, and thus Internet usage may be monitored.**

Any breaches of this Internet usage policy will be treated seriously and will be subject to disciplinary action up to and including dismissal. Breaches may have potential criminal liability and An Gardaí Síochána or other appropriate authorities may be informed.

## Policy - Unnecessary Access to Data

***Curiosity killed the Cat!***

The Law Society of Ireland holds a large amount of personal and sensitive data about its members, students and sometimes members of the public. Under the Data Protection Acts 1988 - 2003 the Society has an obligation to ensure that only staff members with a business need to access a particular set of personal or sensitive data, are allowed to access this data and that they do so only when it is necessary and appropriate for the business of the Law Society.

**What is unnecessary access to data?**

If you are accessing or sharing personal or sensitive data it must be necessary and appropriate for you to access or share this data to carry out a specific work task. Any access to data outside of this criterion will be deemed unnecessary access to data.

***External Example – what actually happened!***

- A Social Welfare officer was disciplined after accessing a well know inter- county GAA player's Social Welfare records numerous times, for no apparent work reason
- A member of the Garda Síochána was found to have accessed her ex-boyfriend's phone records and was disciplined under the Criminal Justice Acts and the Garda Disciplinary Code
- A Revenue staff member was held responsible for a data breach when he accessed his neighbours tax returns unnecessarily
- A bank official was dismissed when he accessed a well-known rugby player's mortgage records and shared his confidential personal data with other people.

***Internal examples – what might happen!***

- Reading minutes of a meeting because it involved your own solicitor or looking up your solicitor's complaints history
- Checking how much money was awarded to your neighbour from the Compensation Fund
- Checking what age a solicitor or student is
- Checking a solicitor's disciplinary record because he is dating your friend
- Looking up the exam results of somebody you went to school with.

**Auditing Compliance**

Access to files containing personal data may be monitored. Spot checks may be carried out and audit trails may be reviewed from time to time.

**Breach of Policy**

Abuse of user access privileges in unnecessarily accessing another person's personal data will be treated as a serious disciplinary matter and dealt with in accordance with the Law Society's disciplinary procedures and may result in a punishment of up to and including dismissal.

## Backups

While controlling physical access to computer equipment is the first line of defence in computer security, making backups is the last line of defence. If the system crashes, or has its security compromised, backups can be used to restore the system to its previous state.

- The IT Staff are responsible for backing up general network directories. Thus, anything saved to the network (H: & I: drives) is automatically backed up for you and stored off site.

- The frequency of backing up your C & D drives is up to you and depends on how important the information is. If the information is critically important, it should be saved to the network for automatic nightly backup. A good rule of thumb is once a week for critical data, once a month for other, if the data is on your PC/laptop only.

## Cyber Security & Safety

Cyber Security has become a staple agenda item at management meetings in The Law Society. Damien Carr is the Law Society Cyber Security Officer.

Grant Thornton conducted a review in August 2016 for the Law Society. In summary, our infrastructure and physical security was rated as average. There has been much improvement since the review recommendations but cyber security and safety is a continuous process. Increasing and improving monitoring tools, improved processes and employee awareness are central to this. Follow up reviews by Grant Thornton will also be carried out.

The Law Society is developing a culture of awareness to Cyber Security. Every Law Society employee has a responsibility as they are our first line of protection and defence. We have the education program called Cybsafe, https://app.cybsafe.com, a program that informs and educates on Cyber Security.

The IT Tips found on the intranet https://www.lawsociety.ie/Intranet/IT/IT-Tips/ will assist in ensuring you are compliant with our Cyber Security policy. The main tips include

- Keeping a clean desk
- Mobile device security
- Ten tips for strong password security
- Social Engineering
- How to Spot a Phishing Email

## Security and Usage Policy for Laptop, Tablets and Smartphones

## Introduction

**This policy describes the controls necessary to minimise information security risks affecting Law Society of Ireland laptops.**

All Law Society of Ireland computer systems face information security risks. Laptop computers, Tablets and Smartphones are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft.

Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (Journalists, firms etc.).

Do not forget that the impacts of such breaches include not just the replacement value of the hardware but also the reputational damage of the Law Society (keeping in mind the reputational damage already suffered by some high-profile organisations) This reputational damage could far outweigh the cost of the equipment itself.

This policy refers to certain other/general information security policies, but the specific information given here is directly relevant to laptops and, in case of conflict, takes precedence over other policies.

## Physical security controls for laptops

The physical security of 'your' laptop is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.

Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. **Never** leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.

If you do store your laptop in your car for any period of time, keep in mind the extreme temperatures range can damage the equipment. The high summer temperatures can cause chip damage, in winter LCD screens can freeze.

Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don't drop it or knock it about! Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

The IT Section have a note of the make, model, serial number and encryption password of your laptop. If it is lost or stolen, notify the Gardaí immediately and inform the It section as soon as practicable (within hours not days, please).

## Virus protection of laptops

Viruses are a major threat to the Law Society and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software MUST be updated at least monthly. The easiest way of doing this is simply to log on to the Law Society network when you are in the office for the automatic update process to run. If you cannot log on for some reason, contact the IT Section for advice on obtaining and installing anti-virus updates. Alternatively, drop it in to the IT Section and we will update it for you.

Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.

Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically but the IT Help/Service Desk can tell you how to initiate manual scans if you wish to be certain.

Report any security incidents (such as virus infections) promptly to the IT Help/Service Desk in order to minimise the damage

Respond immediately to any virus warning message on your computer, or if you suspect a virus (*e.g.* by unusual file activity) by contacting the IT Help/Service Desk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

## Controls against unauthorised access to laptop data

**Your laptop is encrypted, however the encryption is only as good as the secrecy of your password.** Contact the IT Section for further information on laptop encryption. If your laptop is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data. Please also ensure that your password is not written down or kept with the laptop.

You are *personally accountable* for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff.

Corporate laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.

Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

## Other controls for laptops

### *Unauthorized software*

Do not download, install or use unauthorised software programs. Unauthorized software could introduce serious security vulnerabilities into the Law Society networks as well as affecting the working of your laptop. Software packages that permit the computer to be 'remote controlled' (*e.g.* PCanywhere) and 'hacking tools' (*e.g.* network sniffers and password crackers) are explicitly forbidden on Law Society equipment unless they have been explicitly pre-authorised by management for legitimate business purposes.

### *Unlicensed software*

Be careful about software licences. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid and with the permission of the IT section. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and Law Society into disrepute by breaking the law.

*Backups*

Unlike desktop PCs which have their H & I drives backed up automatically by IT, you must take your own backups of data on your laptop. The simplest way to do this is to logon and upload a data from the laptop to the network on a regular basis – ideally every time you bring the laptop into the office. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks *etc*.

**To ensure that off-line backups are encrypted, the IT section will issue relevant staff with encrypted secure USB keys.** Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Off-line backups will save you a lot of heartache and extra work.

*Laws, regulations and policies*

You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet). These are available in the employee handbook.

*Inappropriate materials*

Be sensible! The Law Society will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by email or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, call IT Section to check your spam settings.

## *Health and safety aspects of using laptops*

Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Balancing the laptop on your knees hardly helps the situation! Limit the amount of time you spend using your laptop. Wherever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. If you tend to use the laptop in an office most of the time, you are advised to use a full-sized keyboard, a normal monitor and mouse.

## Security controls for Tablets / Smartphones

- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Law Societies acceptable use policy as outlined.
- All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices whether or not they are actually in use

and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data.

### Do's and Don'ts

- Do create and use a password or pin code to prevent unauthorised access to the laptop, tablet or other mobile device.
- Do turn on 'Find My Phone' (iPhone/iPad) 'Find My Mobile' (Samsung Tablets/Phones)
- Do turn your laptop, tablet or mobile device off and put it in an appropriate carrying case when travelling.
- Do keep all drinks and any other liquids away from your laptop, tablet or mobile device. Any spillage on the device can result in data loss and expensive repairs.
- Do use a Privacy Filter if working in a public place (e.g. on a train, airplane or in a hotel lobby).
- Don't subject the laptop, tablet or mobile device to extreme temperature changes (i.e. don't use or store near radiators or fan heaters). Mobile devices are designed to work within a defined temperature range so exposing them to extreme temperatures (highs or lows) may cause the device to malfunction or behave unpredictably.
- Don't leave the laptop or other mobile device unattended for a long period of time. If you need to leave your desk, put the laptop, tablet or mobile device in a lockable drawer or take it with you. Lock your office door. If you are travelling and cannot keep the laptop, tablet or mobile device with you when it is not in use, then where possible, place the laptop, tablet or mobile device in the
- Hotel safe, or at the very least lock it in your room.

  Don't use your laptop, tablet or mobile device for accessing sensitive Law Society related information in public places if there is a possibility that the information could be viewed by unauthorised individuals and hence le

## Wi-Fi Policy

### 1. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threats.

### 2. Purpose

The purpose of this policy is to secure and protect the information assets owned by The Law Society of Ireland. The Law Society of Ireland provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. The Law Society of Ireland grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to The Law Society of Ireland network. Only **those** wireless infrastructure devices that meet the standards **specified in** this policy or are granted an exception by the Information Security Department are approved for connectivity to a The Law Society of Ireland network.

## 3. Scope

All employees, contractors, consultants, temporary and other workers at The Law Society of Ireland, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of The Law Society of Ireland must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a The Law Society of Ireland Wi-Fi network or reside on a The Law Society of Ireland site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

## 4. Policy

4.1 General Requirements

- All wireless infrastructure devices that reside at a The Law Society of Ireland site and connect to a The Law Society of Ireland Wi-Fi network, or provide access to information classified as The Law Society of Ireland Confidential, or above must abide by The Law Society Internet usage guidelines as specified in our IT Policy

## 5. Policy Compliance

5.1 Compliance Measurement

The Law Society IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by The Law Society IT team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 6. Revision History

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| May 2018 | Martin Kearney | Updated to policy |
| | | |

## Bring Your Own Device (BYOD) Policy

**Acceptable Usage**
The Law Society of Ireland defines acceptable business use as activities that directly or indirectly support the business of The Law Society of Ireland.

The Law Society of Ireland defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

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

Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in outside business activities etc.

The following types of apps are allowed: such as weather, productivity apps, Facebook, etc.

The following apps are not allowed: (apps not downloaded through iTunes or Google Play, etc.)

Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.

The Law Society of Ireland has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

**Devices and Support**
Smartphones including iPhone, Android, Blackberry and Windows phones are allowed.

Tablets including iPad and Android Tablets are allowed.

Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

Devices must be presented to IT for configuration of standard apps, such as office productivity software and security tools, before they can access the network.

**Security**
In order to prevent unauthorised access, devices must be password protected using the features of the device and a password is required to access The Law Society of Ireland Wi-Fi.

The device must lock itself with a password or PIN if it's idle for five minutes.

After five failed login attempts, the device should lock. Employees must contact IT to regain access if it is a Law Society supplied device.

Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

The employee's Law Society supplied device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure

**Risks/Liabilities/Disclaimers**
The Law Society of Ireland reserves the right to disconnect devices or disable services without notification.

Lost or stolen Law Society devices must be reported to the Head of IT and/or the Cyber Security officer within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above and in the IT Policy.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data on their own personal devices.

The Law Society of Ireland reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| | | |
| | | |

## IT Data Security Incident Log

| 1. Contact Information | |
|---|---|
| Full name: | |
| Job title: | |
| Section/Department: | |
| Work phone: | |
| Mobile phone: | |
| E-mail address: | |
| *Additional Contact Information:* | |

**2. Type of Incident** *(Insert X on all that apply)*

| | | | |
|---|---|---|---|
| | Account Compromise *(e.g., Lost Password)* | | Social Engineering *(e.g., Phishing, Scams)* |
| | Denial-of-Service *(Including Distributed)* | | Technical Vulnerability *(e.g., 0-day Attacks)* |
| | Malicious Code *(e.g., Virus, Worm, Trojan)* | | Theft/Loss of Equipment or Media |
| | Misuse of Systems *(e.g., Acceptable Use)* | | |

| | | | |
|---|---|---|---|
| | Reconnaissance *(e.g., Scanning, Probing)* | | Unauthorized Access *(e.g., Systems, Devices)* |
| | Power outage | | Other (please describe below) |
| | System unavailable | | |

**3. Scope of Incident** *(Insert X on all that apply)*

| | |
|---|---|
| | Critical *(e.g., Affects Society-Wide Information Resources)* |
| | High *(e.g., Affects Entire Network or Critical Business or Mission Systems)* |
| | Medium *(e.g., Affects Network Infrastructure, Servers, or Admin Accounts)* |
| | Low *(e.g., Affects Workstations or User Accounts Only)* |
| | Unknown/Other *(Please Describe Below)* |

NOTE: All incidents deemed critical or high require additional notification by phone.

| | |
|---|---|
| Estimated Quantity of Systems Affected: | |
| Estimated Quantity of Users Affected: | |
| Third Parties Involved or Affected:<br><br>*(e.g., Vendors, Contractors, Partners)* | |

*Additional Scope Information:*

**4. Impact of Incident** *(Insert X on all that apply)*

| | | | |
|---|---|---|---|
| | Loss of Access to Services | | Propagation to Other Networks |
| | Loss of Productivity | | Unauthorized Disclosure of Information |
| | Loss of Reputation | | Unauthorized Modification of Information |
| | Loss of Revenue | | Unknown/Other *(Please describe below)* |

| **5. Sensitivity of Affected Data/Information** *(Insert X on all that apply)* | |
|---|---|
| ☐ Critical Information<br>☐ Non-Critical Information<br>☐ Publicly Available Information<br>☐ Financial Information | ☐ Personally Identifiable Information (PII)<br>☐ Intellectual/Copyrighted Information<br>☐ Critical Infrastructure/Key Resources<br>☐ Unknown/Other *(Please Describe Below)* |
| Data Encrypted? | |
| Quantity of Information Affected:<br>*(e.g., File Sizes, Number of Records)* | |
| *Additional Affected Data Information:* | |

| **6. Systems Affected by Incident** *(Provide as much detail if relevant and if possible)* | |
|---|---|
| Attack Sources *(e.g., IP Address, Port)*: | |
| Attack Destinations *(e.g., IP address, Port)*: | |
| IP Addresses of Affected Systems: | |
| Domain Names of Affected Systems: | |
| Primary Functions of Affected Systems:<br>*(e.g., Web Server, Domain Controller)* | |
| Operating Systems of Affected Systems:<br>*(e.g., Version, Service Pack, Configuration)* | |
| Patch Level of Affected Systems:<br>*(e.g., Latest Patches Loaded, Hotfixes)* | |
| Security Software Loaded on Affected Systems:<br>*(e.g., Anti-Virus, Anti-Spyware, Firewall, Versions, Date of Latest Definitions)* | |

| | |
|---|---|
| Physical Location of Affected Systems:<br>*(e.g., State, City, Building, Room, Desk)* | |

| **7. Users Affected by Incident** *(Provide as much detail as possible)* | |
|---|---|
| Names and Job Titles of Affected Users: | |
| System Access Levels or Rights of Affected Users: *(e.g., regular User, Domain Administrator, Root)* | |
| *Additional User Details:* | |

| **8. Timeline of Incident** *(Provide as much detail as possible)* | |
|---|---|
| a. Date and Time When First Detected, Discovered, or Was Notified About the Incident: | |
| b. Date and Time When the Actual Incident Occurred:<br>*(Estimate If Exact Date and Time Unknown)* | |
| c. Date and Time When The Incident Was Contained or When All Affected Systems or Functions Were Restored:<br>*(Use Latest Date and Time)* | |
| Elapsed Time Between the Incident and Discovery:<br>*(e.g., Difference Between a. and b. Above)* | |
| Elapsed Time Between the Discovery and Restoration:<br>*(e.g., Difference Between a. and c. Above)* | |

| **9. Remediation of Incident** *(Provide as much detail as possible)* | |
|---|---|
| Actions Taken To Identify Affected Resources: | |

| | |
|---|---|
| Actions Taken to Remediate Incident: | |
| Actions Planned to Prevent Similar Incidents: | |
| *Additional Remediation Details:* | |