

# **ISPA BEE ISPs/Internet Cafés Training Course**

Course outline & Notes:

Regulations / Legislation for ISPs and Internet Cafes

February 2009

**Contents**

- 1. Introduction..... 3
- 2. Electronic Communications Licensing ..... 4
  - 2.1. Why are there licensing requirements? ..... 4
  - 2.2. When is a licence required?..... 4
  - 2.3. ICASA ..... 5
  - 2.4. The electronic communications licensing framework in South Africa..... 6
  - 2.5. Conclusion ..... 7
- 3. Film and Publications Board (FPB) registration ..... 9
  - 3.1. Registration requirement ..... 9
  - 3.2. Contact the FPB ..... 9
  - 3.3. Child pornography and the child pornography hotline..... 10
- 4. Liability for information passing through your electronic communications systems ..... 11
  - 4.1. How to protect yourself ..... 11
  - 4.2. Codes of Conduct..... 12
  - 4.3. Take down notices ..... 12
  - 4.4. Do you have to monitor the content you are hosting?..... 13
- 5. Spam..... 14
  - 5.1. What is spam?..... 14
  - 5.2. What must you do?..... 14
- 6. Interception and Monitoring..... 15
  - 6.1. Registering your customers ..... 15
  - 6.2. Assisting with investigations ..... 16
- 7. Privacy ..... 17
- 8. Interacting with Law Enforcement Agencies (LEAs) such as the SAPS..... 18
  - 8.1. What do to do when a Law Enforcement Agency or other person requires you to release personal information relating to one of your clients..... 18
  - 8.2. What do you do once a court order has been served on you? ..... 19
  - 8.3. Do you as an ISP have a legal obligation to report illegal or unlawful conduct on the part of one of your customers?..... 19
- 9. Security ..... 20
  - 9.1. Malware ..... 20
  - 9.2. Phishing ..... 20
- PROJECT: Legal & regulatory compliance plan of action ..... 22

## 1. Introduction

While setting up an ISP or an internet café it is important to be aware of the laws and regulations which apply specifically to these kinds of businesses. Previously we looked at some of the legal issues affecting business in general but in this section we will outline some of the issues which specifically affect ISPs and Internet Café's.

We will highlight the legal compliance obligations which must be observed by your new business, including those relating to:

- Electronic communications licensing
- Registration with the Film & Publications Board
- Potential responsibility or liability for information passing through your systems on behalf of your clients
- SPAM
- Interception and monitoring of electronic communications
- Security
- Privacy, and
- Interacting with Law Enforcement Agencies (LEAs) such as the SAPS

**NB.** This area of the law is difficult and changes often and you should do your best to find a competent lawyer or advisor who understands the technical and other issues. Ideally your lawyer should have a good background in commercial law and experience in dealing with ISPs and electronic communications legal issues.

It is also a good idea to consider joining an industry association such as ISPA. Not only are there important legal reasons for doing this but you will also receive information and assistance with regard to how to comply with the different regulations and laws.

**As a new business owner you will have plenty on your hands and this is one area where you will need good advice and support.**

## **2. Electronic Communications Licensing**

The licensing and regulation of ISPs and businesses such as Telkom and MTN is performed by ICASA under the Electronic Communications Act of 2005.

### **2.1. Why are there licensing requirements?**

The Government imposes licensing requirements on businesses in the industry mainly to ensure that:

- Scarce resources such as frequency and numbers can be efficiently allocated and coordinated
- Services are provided in under-serviced and rural areas
- They have authority over licensees, and
- Consumers are protected in their dealings with service providers.

So, in the same way as you would need to apply for a liquor licence in order to operate a bar, you will need to apply for a licence to operate as an internet service provider.

We therefore say that the electronic communications industry is a “regulated” industry.

### **2.2. When is a licence required?**

As a general rule you will need to be licensed whenever your business is involved in carrying communications from one point to another or where you are providing services to your customers across public boundaries.

Think about the main difference between an ISP and an internet café:

- As an ISP you will be providing internet access and email services to your customers wherever they are set up, usually at their work or at home. You will be sending the service to them.
- As an internet café people will be coming to your premises in order to access internet and email services. You will not be providing any service to them other than when they have come to your internet café and paid you for the time they want to spend accessing services. Because your network is regarded as being very small you will not need electronic communications licensing.

So an ISP carrying services to its customers will require electronic communications service licensing while an Internet Café which does not carry services to its customers but rather lets the customers come to them will not require licensing (in other words, it will be regarded as licence exempt).

Summary:

- Before you can start business as an ISP you will require licensing under the Electronic Communications Act
- Internet Café's do not require licensing under the Electronic Communications Act

### 2.3. ICASA

When dealing with licensing issues you will have to approach the Independent Communications Authority of South Africa (ICASA). ICASA is an independent body which is responsible for the regulation of electronic communications in South Africa.

The ICASA Head Office is situated in Johannesburg. There are also regional offices in Cape Town, Bloemfontein, Durban and Port Elizabeth.

Contact details for Head Office are as follows:

*Physical Address*

Blocks A, B, C and D, Pinmill Farm  
164 Katherine Street  
Sandton

*Postal Address:*

Private Bag X10002  
Sandton 2146

Tel: +27 (11) 566 3000/3001

Fax: +27 (11) 444 1919

Email: [info@icasa.org.za](mailto:info@icasa.org.za)

Contact details for the regional offices can be obtained from Head Office or by visiting:

<http://www.icasa.org.za/Content.aspx?Page=153>

Note: When dealing with ICASA you may need to be patient and follow-up regularly to ensure your matter is receiving attention. It will be excellent for your new business if you strike up a positive relationship with ICASA personnel and you should always be polite and positive in your dealings with them.

#### 2.4. The electronic communications licensing framework in South Africa

There are two main categories of licence available under the ECA:

- **Electronic Communications Network Service (ECNS)** licenses: these licenses authorise the holder to roll-out and operate a physical network. This network can be made up of any technology you choose: radio equipment (for a wireless network), copper cabling, fibre optic cabling etc. ECNS licensees can also enter into commercial arrangements with other licensees to allow them to use the electronic communications network owned and operated by the ECNS licensee.
- **Electronic Communications Service (ECS)** licenses: these licenses allow you to provide services to customers over your own or somebody else's network. This will typically be the licence held by an ISP.

Examples:

- Telkom has a telephone or voice network which covers most of South Africa. The network consists of phone lines, switches and other hardware and in order to operate this network Telkom requires an ECNS licence. Telkom then provides voice services to its customers over this network – in order to provide these voice services it will require an ECS licence.
- Vodacom has a GSM network which also covers most of South Africa and consists of their masts and towers which have radio equipment located on them. They will require an ECNS licence in order to own and operate this network and an ECS licence in order to provide their services – voice, data, SMS, MMS etc – over this network.
- An ISP wishes to provide internet connectivity to customers. It does not have its own network (although it may own some hardware) but relies on the services of a network owner and operator such as Telkom (i.e. an ECNS licensee) to carry its services to its customers. In this example the ISP itself does not require an ECNS licence (it does not own and operate the network) but only requires an ECS licence so that it can provide its services to its customers over Telkom's network.

The main licensing distinction is between INFRASTRUCTURE licenses and SERVICE licenses. Whether you will need one or both of these kinds of licenses will depend on the kind of business you want to start.

The ECA breaks down these licence categories into two subcategories:

<b>ECNS licences</b>	<b>Individual ECNS</b>	This allows you to roll out your own network nationwide or across a province.
	<b>Class ECNS</b>	<p>A class ECNS allows you to roll out your own network in a district or local municipality. In other words you will choose to operate in a municipal area and provide access services to consumers in that area.</p> <p>This is the form of licence you would require if you wanted to set up your own network focusing on a smaller area. South Africa has 48 district municipalities and 231 local municipalities as well as 7 metropolitan municipalities.</p>
<b>ECS licences</b>	<b>Individual ECS</b>	<p>This licence allows you to provide services to your customers over the network of an ECNS licensee, including voice or VoIP services which use numbers taken from the National Numbering Plan. Examples of other services that can be provided include:</p> <ul style="list-style-type: none"> <li>• Internet access</li> <li>• Email</li> <li>• Hosting</li> <li>• Protocol conversion</li> <li>• Virtual Private Networks (VPN)</li> <li>• Multi Protocol Labelling Systems (MPLS)</li> </ul> <p>The National Numbering Plan is a document drawn up by ICASA setting out all the different kinds of numbers used in South Africa. A distinction is drawn between geographic – where the number is linked to a specific location, e.g. 011 566 3000 – and non-geographic – where the number is mobile, e.g. 083 000 0000. The number range usually associated with VoIP services is the 087 range.</p>
	<b>Class ECS</b>	This licence allows you to provide the same services as the Individual ECS licence except for voice services requiring numbers from the national numbering plan. If you have one of these licenses you will need to enter into commercial arrangements with one or more ECNS licensees who have the networks to carry your services to your customer.

## 2.5. Conclusion

The simplest way to structure an ISP for licensing and business purposes is to resell the services of a larger upstream ISP. In order to be a reseller of these services – such as internet

connectivity, virtual private networks and email services – you will need to have a class ECS licence.

If, in future, you decide to offer VoIP services then you will need to apply to upgrade this to an individual ECS licence.

Attached you will find:

- Registration form to be completed and sent to ICASA if you require a class ECS or class ECNS licence (Attachment 1)
- The standard terms and conditions of a class ECS licence (i.e. these will be the rules under which you may use your licence) (Attachment 2)

### **3. Film and Publications Board (FPB) registration**

For general information see the FPB's website at <http://www.fpb.gov.za>.

#### **3.1. Registration requirement**

Both ISPs and Internet Cafés are required to register with the Film and Publication Board (FPB) in terms of Section 27A(1)(a) of the Film and Publication Act. This is to assist the FPB in its attempts to provide South Africans with an opportunity to make an informed choice about the kind of movies and other content which they want to see.

Probably the most important issue for the FPB is the fight against child pornography and the exposure of children to pornography and other inappropriate material. You need to take your responsibilities here very seriously and ensure that you take active steps to report child pornography and cooperate with investigations into it.

As an Internet Café owner you will also need to take reasonable measures to ensure that children are not exposed to or able to access pornography on your premises.

As the owner of an ISP or an Internet Café you will receive visits from compliance officers appointed by the FPB who will check that you are properly registered and are complying with any regulations which apply to your business.

The cost of the registration is R825.

A copy of the form required for registration is attached as Attachment 3.

#### **3.2. Contact the FPB**

The FPB's offices are situated at 87 Central Street, Houghton, Johannesburg, 2198

Tel: +27 11 483 0971

Fax: +27 11 483 1084

E-mail: [information@fpb.gov.za](mailto:information@fpb.gov.za)

### **3.3. Child pornography and the child pornography hotline**

The website for the child pornography hotline: <http://www.fpbprochild.org.za/Home.aspx>

The FPB launched the PRO CHILD Hotline in 2008. The primary purpose of the Internet Hotline is to prevent distribution of child pornography (child sexual abuse images) when detected through the internet and there is a team of analysts actively trying to track down child pornography.

The website is also intended to alert Internet Service Providers of the criminal activities, relating to child pornography and or sexual abuse images used /hosted on their servers or distributed through their infrastructure.

The hotline will be available 24hrs a day and 7 days a week to enable members of the public to immediately report discovered child pornography (child sexual abuse images). The Hotline also cooperates closely with Law Enforcement Agencies (LEAs).

#### **4. Liability for information passing through your electronic communications systems**

As an ISP there will be a lot of information flowing through your systems all the time. This information may be emails sent from one person to another, content downloaded from or viewed on the internet or any other content and information resulting from your customers using the services which you provide to them.

The law recognises that it is not fair or reasonable to expect an ISP to be responsible and liable for all of this information. After all the ISP or the people in it are not the ones sending the emails or surfing the Internet, if there is content which is illegal or unlawful then it is really their customers or other people who are responsible. The law also recognises that there is a huge amount of information passing through your systems every hour of every day and that it would be impossible for you to actually monitor all of it.

The Electronic Communications and Transactions Act of 2002 sets out the steps which ISPs need to take to get legal protection against being sued for any of the information which passes through or is stored on their systems or networks.

**Example:**

Your business hosts websites and these websites are available on the Internet. One of your clients writes a story which is not true about someone else and puts it up on their website (which you are hosting). Now the person who is lied about (or defamed) may want to sue your client who wrote the lies but they also be able to sue your business because it helped to put these lies onto the Internet where everyone could see them. A lot of the time they will really try to sue your business because it has more money to pay than the client who published the lies.

##### **4.1. How to protect yourself**

In order to properly protect yourself from being sued as in the above example you need to join an industry association which is recognised by the Department of Communications as an Industry Representative Body (IRB).

Although the Department has not recognised any association as an IRB yet ISPA is hopeful that it will be recognised before the end of 2008.

## 4.2. Codes of Conduct

Once you have joined an IRB you will be expected to comply with its Code of Conduct and to agree to be bound by its disciplinary procedures.

A Code of Conduct usually sets out rules about

- Being professional in your dealings with customers
- Not sending spam and taking steps to stop your systems from being used by others to send spam
- Respecting the privacy of your customers and their communications
- The protection of children
- How to deal with illegal and unlawful content

Have a look at ISPA's Code of Conduct: [http://www.ispa.org.za/code/code\\_of\\_conduct.shtml](http://www.ispa.org.za/code/code_of_conduct.shtml).

Think about all the items which you will need to take into account in running your business.

- How do you train your staff to be professional and to respect your customer's privacy?
- If you are running an Internet Café how will you make sure that children are not able to access inappropriate content such as pornography? How will you make sure that they are not exposed to other people viewing this content?
- If you are running an ISP how will you deal with spam and make sure that people do not use your systems for the sending of spam?

ISPA's Code of Conduct makes provision for complaints to be laid with ISPA in respect of one of its members (or ISPA itself can lodge a complaint). This may lead to an Adjudicator being requested to decide whether the member is in breach of the Code of Conduct or not.

The Adjudicator may, if he or she finds there has been a breach, impose fines or order content to be taken down. If the breach is serious the member may be suspended or expelled from ISPA and the matter may be reported to the SAPS.

## 4.3. Take down notices

Think about the example above about the client's website your ISP is hosting. How does the person who has been lied about get the lies removed from the Internet as quickly as possible?

The best way to do this is to send a document called a Take Down Notice. This Notice will contain

information about the material which should be removed from the Internet and also say that the person who want this material taken down is acting in good faith.

If you are a member of an IRB you will be best advised to let the IRB be your agent who will receive take down notices on your behalf. An IRB like ISPA will then be able to make sure that you are aware of the problem and advise on you on how to proceed.

If you are a member of an IRB and you receive a Take Down Notice which contains all of the information it should have then you should generally take the material down or suspend access to it and you will be safe from being sued by your client.

#### **4.4. Do you have to monitor the content you are hosting?**

Remember that you do not have to sit and check to make sure that all of the websites which you host do not contain anything which they shouldn't, such as the lies in our example above. How are you to know that they are lies in any case?

But always remember that if you become aware of any illegal content such as child pornography then you must report it to the authorities as quickly as possible.

## 5. Spam

Spam is one of the biggest challenges to ISPs, who have to spend a lot of money and time fighting it and trying to prevent it from going through to their customers.

Every ISP has a duty to participate in the fight against spam and to make sure that its systems and networks are not used for the sending of spam.

### 5.1. What is spam?

Unfortunately there are different definitions and lots of arguments about what is and what isn't spam. As an ISP you will simply be concerned with people who are sending huge amounts of emails to your customers and others who have not asked for this email (i.e. it is unsolicited). This is referred to as bulk commercial mail and it can cost your business dearly in bandwidth costs and lost clients if it is not properly managed.

For more information on spam you can visit <http://www.ispa.org.za/spam/index.shtml>.

### 5.2. What must you do?

If you belong to an Industry Representative Body (IRB) then the Code of Conduct will require that you take steps to prevent the sending of spam over your network.

ISPA's Code of Conduct on spam:

#### **E. Unsolicited communications ("spam")**

14. ISPA members must not send or promote the sending of unsolicited bulk email and must take reasonable measures to ensure that their networks are not used by others for this purpose. ISPA members must also comply with the provisions of section 45(1) of the ECT Act.
15. ISPA members must provide a facility for dealing with complaints regarding unsolicited bulk email and unsolicited commercial communications that do not comply with the provisions of section 45(1) of the ECT Act originating from their networks and must react expeditiously to complaints received.

## 6. Interception and Monitoring

The South African Government has passed various laws aimed at assisting the Law Enforcement Authorities (LEAs) to fight against crime and terrorism by intercepting and monitoring electronic communications.

### 6.1. Registering your customers

There is currently uncertainty as to the exact steps to be taken when you sign up and register your customers. ISPs are required to act in a similar way to banks when they are opening up new accounts and have to obtain certain information from their customers before this can be done. This is called a Know Your Customer obligation.

It is recommended that you collect at least the following information from your customers when you sign them up:

#### *Customers who are individual people (not businesses)*

- name,
- identity number
- residential and postal or business address;
- a certified photocopy of the identity document where the customer's name, photograph and identity number appear (a certified copy is a copy which has been signed by a Commissioner of Oaths such as an attorney or bank manager);

#### *Businesses (Companies, CCs, Trusts etc)*

- name, identity number & residential and postal or business address of the person representing the business;
- name of the business,
- business address;
- registration number (if the business is registered)
- a certified copy of the identity document of the person representing the business, where their name, photograph and identity number appear;
- a certified photocopy of the business letterhead;

You are required to keep all of this information and the certified copies in a safe place. If they are required by the SAPS or other LEAs then you must be able to produce them.

## 6.2. Assisting with investigations

You may in the course of running your business be approached by SAPS or another LEA to assist them with a criminal investigation. As always ensure that you give them your full cooperation.

Example:

Your ISP has a client Mr X who is suspected by SAPS of being involved in criminal activities. They also suspect that he using email messages to his accomplices to plan his crimes. In order to catch him in the middle of committing a crime they wish to see the emails which he has already sent and the ones which he is going to send for the next two weeks.

SAPS will need to go to a Judge and get what is called an Interception Direction which allows them to intercept and monitor Mr X's communications. They may then approach you and ask for your assistance in implementing the monitoring and interception.

For as long as you are a small operation or acting as a reseller this is unlikely to happen. If it does then the Interception Centre will assist you in complying with your obligations.

Interception and monitoring is regulated under the Regulation of Interception of Communications and Provision of Communication-related Information Act. If you want more information please read the ISPA Advisory which you can find at

<http://www.ispa.org.za/regcom/advisories/advisory10.shtml>.

## 7. Privacy

It is important to remember that your customers have a right to privacy and that you should at all times respect this right.

Every ISP and Internet Café should have an Acceptable Use Policy (AUP). This is a legal agreement entered into between your business and its customers and which sets out the rules under which they can use the services which you provide. Your AUP should be drafted or reviewed by your attorney or advisor and will have to fit in with the Code of Conduct of any Industry Representative Body which you are a member of.

Your AUP should make it clear how you will deal with the personal information relating to your customers and it should set out the circumstances under which you will release it (usually only with your customer's consent or where there is a court order requiring you to release it).

This personal information can include:

- the content of email messages
- information about the surfing habits of your customers
- IP addresses assigned to your clients
- any information about your customer such as their name, age, address, identity number and the like.

If you have an ECS licence then your licence will require that you take steps to respect your clients' privacy. It is likely that South Africa will get a new law relating to privacy of electronic communications in the very near future and that there will be new compliance obligations for ISPs and Internet Café's.

## 8. Interacting with Law Enforcement Agencies (LEAs) such as the SAPS

This section covers the correct procedure to follow when a Law Enforcement Agency (LEA) or another person wants personal information regarding one of your customers.

### 8.1. What do to do when a Law Enforcement Agency or other person requires you to release personal information relating to one of your clients

As an ISP or an Internet Cafe you will get visited by organisations and Law Enforcement Agencies (LEAs) who wish to obtain information from you regarding one of your customers. This may be as a result of an investigation into a number of issues, including

- child pornography;
- an alleged online copyright infringement;
- alleged bandwidth theft;
- the implementation of an interception under the Regulation of Interception of Communications Act (RICA); and
- an alleged offence under Chapter 13 of the Electronic Communications and Transactions Act (Unauthorised access to, interception of or interference with data / Computer-related extortion, fraud and forgery).

As a general rule do not hand over any personal information regarding your customers unless you have been presented with a warrant or subpoena signed by a Magistrate or a Judge and presented by a member of the SAPS.

Always cooperate fully with the LEAs. If necessary explain that you are required to act within the scope of the law and your contracts with your customers and that both of these require that you must have an appropriate court order before you can release personal information.

**If you release this information without proper authority then you will probably be breaking the law.**

**8.2. What do you do once a court order has been served on you?**

As quickly as you can obtain the information that has been requested. Follow what has been set out in the court order as closely as possible.

Generally you will not actually be required to be present in court to present the information – you can simply phone the person who's contact details appears on the court order (which will usually be a police officer) and make arrangements to provide the information to them.

**8.3. Do you as an ISP have a legal obligation to report illegal or unlawful conduct on the part of one of your customers?**

Remember that as an ISP you have no general obligation to monitor the information which passes through or is stored on your systems (section 78 of the Electronic Communications and Transactions Act).

**But once you become aware of illegal content, especially child pornography, you are required to report it immediately and cooperate with the LEAs to the best of your ability.**

## 9. Security

While the majority of the steps which you take to ensure that your system remains secure and to protect your customers from security threats will be technological or software-based, there are some legal issues to be aware of.

### 9.1. Malware

Malware, or malicious software, is software designed to infiltrate or damage a computer system and includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.

A failure to maintain industry standards in ensuring the system of, for example, an Internet Café, may lead to your customers falling prey to Internet criminals and fraudsters. This has happened in South Africa where keystroke loggers, simple programs which records the keys pressed on a keyboard, have been installed on Internet Café computers, causing the banking of customers to be compromised and used to steal money.

It is important to

- Educate your customers about the need to take steps to secure their own computer systems by using a reputable and updated anti-malware programme
- Educate your customers about the dangers of doing their online banking at a public computer (such as a computer in an Internet Café) and ensure that they are aware that, if they choose to do this, it will be at their own risk
- Ensure that you have the ability or the personnel to properly manage the security of your network.

### 9.2. Phishing

Phishing occurs where criminals attempt to acquire sensitive information such as usernames, passwords and credit card details by pretending to be a bank or another trusted entity. Phishing is typically carried out by e-mail or instant messaging. A typical email would use letterheads and language designed to make the recipient believe it is an official communication. The recipient is often asked to update their details (e.g. their banking password) by clicking on a link which takes them to a replica of the bank's website.

Make sure that your customers are aware of the dangers of phishing scams. Consider putting up posters in your Internet Café or making information available on your website which explains the dangers of email and the Internet in clear and simple terms.

## **PROJECT: Legal & regulatory compliance plan of action**

Make a list of the regulatory compliance issues which you need to consider when you are at the planning stage of setting up your ISP or Internet café. In your list:

- Identify the government or other agencies you will need to interact with
- Distinguish between those things you will do yourself and those that you will ask a lawyer to help you with.
- Wherever possible list the cost attached to any compliance issue and indicate whether this is a once-off or a recurring cost. You should create a budget for dealing with these compliance and regulatory matters. Use the Internet to figure out how much the membership fees of industry associations are

Visit the FPB and PRO CHILD Hotline websites and read about the fight against child pornography and the need to protect young people from being exposed to all kinds of pornography. Make a list of the things that your business needs to do to ensure that you and your business are participating in the fight against child pornography and what steps you can take to prevent children who come to your Internet Café or use your ISP's services from seeing pornography.