

*DATA PROTECTION (JERSEY) LAW 2005*

***SOCIAL NETWORKING WEBSITES:  
A GUIDE FOR USERS AND  
PROVIDERS***





## Part 1



## Guidance for Users

# Using social networking sites safely

Social networking websites, where people can meet, chat and message each other online are used by millions of people all over the world. Some people are worried about how safe it is to use the internet to share personal details in this way. A website which collects information from you has an obligation to, among other things, keep the information safe, keep it up to date and not use it in a way you might not expect. Providers of social networking sites have a responsibility to ensure that people using the site can do so safely. This means that the site should have readily available information and guidance for users in respect of helping maintain their right to keep information about themselves private, such as privacy policies and helpline facilities, for example.

However, users also have a role to play in protecting their own privacy. This guidance will encourage safe use of these sites and help you enjoy the benefits of being online while reducing the risks of posting information about yourself on the net.

## What is social networking?

There are many different types of social networking sites and they all work in slightly different ways but basically, they help you keep in touch with friends, get to know new people online or store and share pictures, music and experiences with other people.

If you use a networking site, chat in a forum, or if you use internet dating then you may be putting personal information online so this guidance may be useful to you too.

On most sites, you will create a profile for yourself. A profile may just be a username and a contact address but might include a photo. Your profile will often be a description of you, the things you enjoy doing, the music you like or even videos you have made. It will often have links to your online friends' profiles.



## Taking care of personal information

The reason why social networking sites are so popular is because they make it easy to share information with so many people: it's easy, for example, to let your friends see your holiday photos before you even get back home, or, when you do get home, you can instantly look up the profiles of the people you met on holiday and send them a message. But it's important to remember that any information you post on a site could be public and may be seen by lots of people.

This means you have to be careful about what you reveal about yourself to other users. If information you post is seen by more people than you expect, this could pose a risk to your privacy or even your personal safety. Once information is 'out there' you might not be able to control what happens to it: your profile may be seen by thousands of strangers, parts of a website may be 'public spaces' so what you say on them is also public, and not everyone will agree with what you write. Also, it can be easy for others to copy your pictures, even alter them, and send them to people you don't know.



So, before you create a profile, post a picture or tell the online world what you got up to today, have a think about the following and consider whether you are being as safe in the online world as you would be in the offline world.

### Are you using the right sort of site?

People network for all sorts of reasons and there are different sites to suit their needs. You need to make sure that the sites you use are the right ones for you. For example, some sites are aimed at specific age groups so you need to be sure that other users are in an age group you are comfortable with.

Also, you may find it helpful to chat about how you and others have coped with a difficult time in your life such as an illness or the death of a family member. The internet can be a good way of doing this but you need to find out if the site you use allows you to talk about these issues safely and with people who understand your situation. For example, the site may allow you to restrict access to certain personal information.

## Do you know how the site works?

Most sites let you control how public or private your profile or information about what you have been doing on the site is. These controls are often called 'privacy settings'. Choose a site that gives you as much choice as possible over who is able to find your profile and how much information they can see.

While on some sites privacy settings are automatically set at their most 'private level – in other words, if you do nothing, your profile and activity will be hidden – on others, all your information could be seen by other users unless you take action. On the site you want to use, check out how it works by viewing any profile settings and identify the privacy settings before you start building your profile. Set the privacy level as strictly as you can – remember, you can always make more information available to more people as you get used to the site and the other users but you can't take information back from a stranger once they've seen it.

Also, to learn more about a site's privacy procedures and settings it's a good idea to read any privacy policies and user agreements regularly. This will help you understand how the site operators use your personal information, for example whether they pass it on so other people can send you marketing.

## Would you want a stranger knowing this about you?

You might think that only your friends would want to look at and use information about you but you should always be careful with the information you post. Little bits of information about you can be used by others to build up a picture of who you are. In social networking, this is often a good thing as it helps you get to know people quickly and work out who likes the same things as you. But sometimes you might be revealing more about yourself than you would like and this could be misused.



For example, it might seem obvious to suggest that you should never reveal information such as your home address or telephone numbers to strangers but people still do – some people even give out their passwords allowing others the chance to access and alter their profile.

Make sure your password is safe by avoiding ones which others might guess (such as the name of your dog or the football team you support) and keeping it secret. Change it regularly. You may use some of this information as passwords for other things such as internet banking so think carefully before you put it in your profile.

You might have decided not to allow people to see how old you are until you get to know them. So make sure that any email address you give out does not reveal the year you were born such as [jimjones1986@emailaddress.com](mailto:jimjones1986@emailaddress.com). It's a good idea to have one email address that you only use for social networking; that way, until you get to know someone, you don't have to tell them any of your other contact details.

Also, if you don't want people you meet online to work out your 'real life' location, take care not to give out information which would reveal where you are likely to be at certain times such as the school you go to, a work email address or even telling people that you work in 'Café Society in town on a Saturday morning'. Always remember that your personal safety offline can be affected by what you tell people online.

## What will other users think?

It's not just a matter of personal safety. You should also remember that what seems frivolous or even trivial to you and your friends could damage your reputation when seen by others. For example, there are stories of how pictures taken at parties and posted on a profile have caused embarrassment, or worse, when seen by parents, teachers, employers and law enforcement authorities. Before you post something, ask yourself what impression someone would get from seeing your web presence. If you applied for a job, would you want the people interviewing you to have seen everything on your profile?

## Who else is online?

One of the attractive things about social networking is that it gives you the chance to meet people you'd never have met in the offline world. But remember that online friendships don't always work in the same way as offline ones. Before sharing personal information, you need to judge whether you really trust someone with your contact details or private thoughts. Also, the dozens of people you meet online will also have met dozens of other people as well as you and all those people will have other online friends. Would you be happy for hundreds of people to be told all about your private life? If not make sure your friends know how to treat the information you share with them before you share it.

It's just as important to remember that your online friends will also have their own expectations of privacy and how they would want you to treat their personal details. Just because they have told you something does not mean they want you to share it with people you know but they don't.

## Finally...

Most people use and enjoy social networking sites safely and this guidance is not meant to scare anyone. If something starts to spoil your enjoyment – unwanted attention, offensive comments – most sites allow you to report inappropriate activity. Make sure you read and understand how to do this.

Social networking sites are a useful way to meet people and keep in touch with friends and they can be a privacy friendly way to socialise – sites should allow you to control who you contact, who contacts you and what information, if any, they find out about you. Make sure you control access to yourself online you as you would offline, hide details you think are sensitive or simply don't post them at all. Above all, learn how the sites you are using work and how you can use them safely.



## Part 2



## Guidance for Providers

# Protecting the user

As a provider of a social networking website, there are a huge number of factors to consider both during the development stages and once the site is publicly available on the internet. Protecting the user's privacy should feature highly on this list as it is this area that will ultimately attract users to the site and promote confidence in its ability to use safely.

This guidance is intended to cover the key areas which need to be considered to ensure the safe use of the site and protect the user's right to privacy.

## Regulatory requirements

The collection, use and disclosure of personal information by data controllers in Jersey is regulated by the Data Protection (Jersey) Law 2005 ("the Law"). Amongst other things, a data controller has a legal obligation to ensure that the collection, use and disclosure of personal information is carried out in such a way that it complies with the Law and the eight data protection principles.

Whilst other more detailed guidance published by the Office of the Data Protection Commissioner is available in relation to regulatory requirements, there are a number of key relevant areas to consider in the context of social networking websites:

### **1. Notification:**

The Law requires all data controllers who hold personal information to Notify with the Commissioner, unless you can apply an exemption from Notification.

- Is your organisation (the website provider) Notified with the Office of the Data Protection Commissioner? If not, do you know which exemption from Notification your organisation is relying upon?

### **2. Data collection:**

The eight data protection Principles set enforceable standards for all types of data processing. (See the Commissioner's Guidance document GD1 – The Data Protection Principles). Compliance with the Principles will ensure information is collected:

1. Fairly and lawfully;
2. processed for specific purposes;
3. is relevant for the purpose required;
4. is accurate and kept up to date;
5. is retained for no longer than is necessary;
6. is held in accordance with the rights of individuals under the Law;
7. is kept securely;
8. sets requirements for any overseas transfers.

As a data controller, and in order to comply with the above Principles, you should be asking yourself questions such as:

- How do I collect information from users? Is it collected fairly and lawfully?
- What purpose(s) am I collecting the information for?
- How is that information stored and who has access to it?
- How secure is that information? How do I keep it as secure as possible?
- How do I keep the information up to date?
- How long will I be keeping user information?
- Will I need to share the information with anyone else? If so, who?
- Do I have a data protection policy on my site that communicates how I do all these things to users of the site?

## Protecting privacy

How you keep information about your users private will be key to the success of the site. As well as the clear reputational advantages of having a social networking site which publicly prides itself on protecting its user's privacy, a privacy-friendly site will ultimately attract more users than a site which pays little regard to the rights of individuals wishing to use the site.

There are an infinite number of ways in which a website provider can safeguard the rights of their users and help to protect their privacy.

### 1. Privacy policies

- Do you have a Privacy Policy and/or User Agreement on your site?

The Office of the Data Protection Commissioner has issued separate guidance on the issue of Privacy Policies and what they should include. Please see Guidance document GD16 – Guidance for Privacy Statements on Websites.

In addition, a User Agreement would obtain consent from individuals who, upon registration with the site, would need to agree to certain processing taking place, for example, sharing certain information with marketing companies. The provider however must determine whether or not the processing is absolutely necessary to allow use of the site, and if not, provide the appropriate facility to allow the user to opt out of such processing.

### 2. Restricting access to profiles – Privacy settings

- Does the site allow people to restrict access to certain personal information?

Many social networking websites allow users to take control of who can and cannot have access to certain information in their profile. Give the user as much choice as possible over who is able to find a users profile and how much information they can see.

- What is the default on the privacy settings you offer?

Some sites start out on the basis that everything is private and allow the user to take control over what information they are happy to be fully accessible. Other sites do the opposite and start with an open book with everything available for all to see. Clearly the former approach would be considered best practice, but the key is to ensure that the user is fully aware of what the default position is before they start adding information to a publicly accessible profile.

### 3. Inappropriate content or activity

- Do you monitor site activity for inappropriate use or content?
- Does your site allow users to report inappropriate activity or content?
- Does your site make it clear what constitutes inappropriate activity or content as part of its terms of use?
- What sanctions do you impose if a registered user is found to have contravened the terms of use?

Having the ability to report inappropriate use, activity or content on your site is essential to maintaining user confidence. If a user doesn't think you are taking their privacy or personal security seriously, they will find another website provider that does.

Finally...

Clear privacy policies and privacy rules are essential to any social networking website and providers should be providing as much information about what happens to user's personal information, including precisely what information is used for and how long the information will be retained. It is not always obvious to the user that their personal information could be kept for a long time and in some cases indefinitely, so once again this is something that should be communicated on the site to the user.

The greater the transparency and information provided to the user, the better the chances of a user having a much safer and more enjoyable experience on your website.



# CONTACT THE COMMISSIONER:

## **Enquiries and Publication Requests:**

T: 01534 441064

F: 01534 441065

E-Mail: [dataprotection@gov.je](mailto:dataprotection@gov.je)

W: [www.dataprotection@gov.je](http://www.dataprotection@gov.je)

## **Office of the Data Protection Commissioner**

Morier House

Halkett Place

St. Helier

Jersey

JE11DD

