MyRuby

# Data Protection Policy

| | |
|---|---|
| Title: | Data Protection Policy |
| Author's Name: | Andrew Perillo |
| Version No.: | 1.2 |
| Approved By: | Natalie Perillo |
| Approval Date: | 30.01.2014 |
| Planned Review Date: | 01.02.2015 |

# Data Protection Policy

**MYRUBY RESPECTS THE PRIVACY OF EVERY INDIVIDUAL WHO COMES INTO CONTACT WITH THE MYRUBY SERVICE.**

This Privacy Policy explains how MyRuby Limited collects and processes personally identifiable information. We operate within Data Protection and Privacy legislation in the UK and are fully registered under the UK Data Protection Act 1998.

MyRuby Limited and its employees agree to conduct their business according to the following charter:

## For Computer Security:

- Our computer network and systems are protected by a firewall and up to date virus-checking on all computers.
- The latest software patches and security updates to cover vulnerabilities are regularly uploaded to our systems.
- We only allow our staff to access the information they need to do their job.
- Where possible we use software systems that encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- We take regular back-ups of the information on our computer systems and keep them in a secure, fireproof safe so that should our computers become unusable we don't lose the information.
- We securely remove all personal information before disposing of old computers by using software specifically designed for the task or by destroying the hard disk.
- All of our systems are protected by Anti-spyware to monitor and protect from spyware threats.
- Where we are using third party or cloud based systems we ensure that our suppliers/parties sign up to similar levels of security and are listed on the data protection register and/or also a certified licensee of the TRUSTe EU Safe Harbor Seal and abide by the EU Safe Harbor Framework.
- We have a policy of using strong passwords - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters, such as the asterisk or currency symbols.

## For Using Emails Securely:

- We use regularly updated spam and virus filtering software on our servers and PCs.
- We consider whether the content of the email should be encrypted or password protected and if it is of a particularly sensitive nature we use a secure ftp site to transfer data to clients.
- We advise staff that if they want to send an email to a recipient without revealing their address to other recipients, to make sure they use blind carbon copy (bcc), not carbon copy (cc).
- Group email addresses are used carefully. Staff are advised to check who is in the group and make sure they really want to send the message to everyone.

## For Using Faxes Securely:

- We consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. We make sure we only send the information that is required.
- We make sure that we double check the fax number we are using. If a number is used regularly we will add it to a directory of previously verified numbers to avoid misdialing.
- If the fax is of a confidential nature we will check that the fax we are sending to is not accessible by unauthorised individuals such as in an open plan office.
- If appropriate and the fax is sensitive, we will call the recipient and ask them to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- We will call or email to make sure the whole document has been received safely.
- Where necessary we will use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

## For Other Security:

- We regularly check our physically storage of data to check whether it needs to be kept or can be securely destroyed.
- We shred all of our confidential paper waste.
- Our building and car park site are protected by 24HR Monitored CCTV and alarm systems.
- Main access to our building is controlled by time-lock which is secured from 6pm to 8am Monday to Friday and at weekends and bank holidays. A coded key fob is required to gain access.
- Confidentiality of information that employees may come into contact with is part of induction training and regularly included in our in-house training.
- Confidentiality of information is included in our employee contracts so that they can be prosecuted if they deliberately give out personal details without permission.

## How To Contact Us:

You may address all communications regarding this policy to The Data Director, MyRuby Limited, 3-5 The Centre, The Crescent, Colchester Business Park, Colchester CO4 9QQ. Please include your name, address and telephone number or e-mail in all communications and state clearly the nature of your query.

## Changes To Our Privacy Policy:

This privacy policy is effective as of 1st January 2014. If we make any changes to our Policy, we will post the updated Policy and the revision date on the Privacy Policy page of www.myruby.co.uk. Users who have authorised e-mail communication may be notified via e-mail of any material changes to the Policy.