Data Protection 101

Note: Whilst this document refers mostly to laws in EU countries, all of the principles are relevant anywhere in the world.

When you run a Dojo you will amass a lot of information from various sources about people who attend or are interested in your Dojo, from information about the kids who register each week to information about mentors from their background checks. When handling this information it's important to keep in mind that these people have trusted you to keep this information safe, and as such it's important to respect it and make sure that it is kept secure.

8 Rules of Data Protection

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit, lawful purposes
3. Use and disclose it only in ways compatible with those purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to an individual, on request

Obtain and process information fairly

It is important that you only collect the information that you need to run your Dojo. The person must be aware that you are collecting it, and understand what it will be used for. In the case of a child's information, you should make sure the parent also understands that you are collecting it and what the data will be used for.

Keep it only for one or more specified, explicit, lawful purposes

In general a person should know the reason/s why you are collecting and retaining their data. The purpose for which the data is being collected should be a lawful one. You should be aware of the different sets of data which you keep and the specific purpose of each.

Use and disclose it only in ways compatible with these purposes

You should only use the information you collect for the purpose you collected it for. For example, you shouldn't use a phone number which was only given as an "emergency contact" to send promotional text messages advertising the sessions. This purpose should also be made obvious to the person providing the information.

Keep it safe and secure

You should keep data physically and digitally safe and secure. Use encryption where data is stored "at rest" on laptops, whole disk encryption like BitLocker on Windows or FileVault on Mac should be used. If there are cabinets where you keep physical files, such as Garda Vetting forms, they should be locked securely when they aren't in use.

You should also make sure that only people who need access to the data have access to it. Mentors, for example, probably do not need access to all email addresses on your mailing list.

Keep it accurate, complete and up-to-date

You should keep the data up-to-date, and ensure that people have the opportunity and ability to update the data where they need to.

Ensure that it is adequate, relevant and not excessive

Only keep information that you need. For example, you should not collect details such as a child's race or religion unless it is relevant to the activity that you are doing.

Retain it for no longer than is necessary for the purpose or purposes

Do not hold data infinitely. You should destroy any data you hold once it becomes unnecessary to hold the information for the purpose that you originally collected it. For example, if someone who is not otherwise involved wishes to be removed from a mailing list you should delete their personal information.

Give a copy of his/her personal data to an individual, on request

When someone asks for a copy of their information you should provide them with it. This does not extend to data relating to another person.

Intended for RP Pilot Participants **Last Modified: 05/09/2014**