

Data

Collection, Protection,
Storage and Use



Data Protection

Everyone has a legal obligation to protect an individual's data.

Personal Identifiable Information (PII) is defined as information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context.

There are two types of data loss:

Accidental: Human error or carelessness can lead to accidental loss, including something as simple as sending an email attachment containing PII to the wrong recipient

Malicious: data breaches that are deliberate, either by individuals or through external attacks

If we all apply some simple checks on how we deal with data, we will reduce the chance of either occurring.

What is Personal Identifiable Information?

Types of PII

- Date of birth
- Country, county or city of residence
- Credit card details
- Medical records
- Age
- Telephone numbers
- Email addresses
- Gender
- Race
- Criminal record



Collection of Personal Data

The Official bit...

- shall be collected and used fairly and inside the law
- shall be obtained only for specified purposes and shall only be used for those purposes
 - *e.g. you cannot collect data for player registration and then use it to advertise a coaching session*
- shall be adequate, relevant and not excessive
 - *don't collect and hold data for the sake of it, collect it for a purpose*
- shall be accurate and, where necessary, kept up to date
- shall not be kept for longer than is necessary for what is was collected for
 - *don't hold on to data unnecessarily for an extended period of time, suggested no longer than a couple of years*
- shall be kept safe and secure
- shall not be transferred outside of the European Economic Area (that's the EU plus some small European countries), unless destination territory has similar data protection rules

Tips for Protecting PII

A few steps to improve data protection whilst storing and moving data...

Storing Data

- Do not store PII files on laptops / desktops where possible
- If a personal device with access to PII is lost or stolen report it immediately
- If you do store PII on a computer or electronic storage device (USB stick / CD), ensure entry to it is password protected
- All hard copies or electronic storage devices of PII must be stored in a locked environment (desk drawer or cupboard)
- Where possible, shred any hard copies of PII information immediately after use

Moving Data

- Ideally use a secure FTP site (such as Filezilla) to transfer PII data files
- If emailing, always password protect PII files and send the password in a separate communication
- If using flash drives, hard drives, CD's, USB sticks use password protection
- Only send PII to people that absolutely require it & double check the destination before sending!

What is FTP - (File Transfer Protocol)?

It is a system used to transfer files over the Internet. People commonly use FTP to make files available for others to download. Access can be by invite only and the information can be password protected.

FAQ – Examples of use

I have lots of data about players within my club, how is best for me to save this?

Only store what you absolutely need to. The best way to store this is within MyNet, as this is a secure environment. If you need to keep this information yourself, then use a computer or electronic storage device, but on all occasions, password protect access to the files and where possible, store the items in a lockable cupboard / drawer.

When collecting data, do I need parental consent for children? *An individual is considered able to give their consent if they understand what they are being asked. Generally, this is considered to be anyone over 12 years of age, though depending upon the sensitivity of the information, you may feel that you would like to get parental consent above this age also. This is for you to judge on a case-by-case basis, but we would advise that where possible you do this for anyone under the age of 18.*

Can I share a list of athletes that were selected for regional academy with other coaches and the committee - it includes their parents details as well as their DOB, clothes sizes and which school they attend? *You can use the data that you hold for the purpose it was given. Is it relevant to send all of the information held to any or all of the recipients? Only send what is relevant and required. If it is, then via an FTP site or by email with password protection on all files and the password sent separately.*

FAQ – Examples of use

When I coach a session I know I need emergency contact details in case there is an accident/injury. I usually leave this information on the bench at the side of the sports hall. The ideal way to have access to this information is on an electronic device, which is password protected (a mobile phone most obviously). If this is not available, a hard copy of the very least amount of emergency data required should be secured, most effectively by keeping it on your person. Do not add this information to a publically available register at the event, keep it separately with you.

I am on the county committee, can an NDO, Regional Co-ordinator or another member of EN staff send me details of people who have been on a coaching course just so we have this information? If the individuals have given their permission to be contacted for this purpose then this is fine, but this should only be used for the purpose that it was collected and within a acceptable time period so as to be relevant. If there is no specific or relevant reason to hold the data, you are only putting yourself at further risk by doing so.

I have 10 players at a tournament and the organisers need their name, DoB and contact details. What should I do?

It is OK to send this information, though the combination of this data will make these people identifiable. Either do so via an FTP site or if sending by email, ensure that the Excel/Word document is password protected, and send the password separately.

FAQ – Examples of use

I keep all my netball files on a memory stick as a back up in case my laptop breaks and so I can take everything to a committee meeting – is this OK? *It is fine to do this, particularly as a back-up solution, though all files including PII should be password protected, whether on your computer or memory stick. If taking the information to a meeting is essential to the purpose of the meeting then this is fine, but if the information is being taken ‘just in case’, we would suggest that you reduce the risk of a loss of data and keep the files locked away in a safe place.*

Where should I direct people for more information on data protection so we can carry on doing our roles but in the knowledge that it’s all safe? *There are many user friendly guides online, however be careful that they are up-to-date, as something published a year ago could now be superseded (guidelines are moving that fast!). For the definitive answers, the best place to go is to www.ico.org.uk, the website of the Information Commissioners Office.*

For further guidance, please email info@englandnetball.co.uk and a member of staff will respond to your question