

Clarborough & Welham IT Group

Data Protection Policy

This policy document supersedes all previous versions.

This policy document should always be read in the light of the current Data Protection Act or subsequent UK Parliamentary instruments as appropriate. At the time of writing, the appropriate Acts are **Data Protection Acts 1988 and 2003**.

Within this document 'IT Group' shall mean Clarborough & Welham IT Group.

These Acts require that we must ...

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

According to the advice obtained on official sites, our organisation is not required to register with the Data Protection Commissioner.

The key elements of the above requirements that we need to address are:

1. Periodically inform those from whom we have obtained data, that we hold it.
2. Periodically ensure that our data is up-to-date.
3. Ensure the data is only adequate for purpose – which in IT Group case means appropriate for emergency or other basic contact details.
4. Keep data safe such that it cannot fall into third party hands.
5. Determine which members of our committee should have access to the data and under what conditions (i.e. time frame, etc).
6. Delete the data once it is no longer relevant.
7. Have mechanism in place for members to review their data.

To these ends, the IT Group will...

1. inform members at the beginning of each block of classes that we hold the data that they provided on their Enrolment Form the purpose of which was emergency contact or provision information.
2. not pass any personal data to any third party unless required to by law.
3. regularly check with members that their data has not changed since the last check.
4. only enter data comprising **name, address, telephone number** (including **mobile** if appropriate) and **e-mail address**) into a spreadsheet for the above purposes.
5. stored the above spreadsheets on USB Flash drive(s) and NOT on any computer storage system. The Flash drive(s) will be stored in a secure location, remote from computer(s).
6. ensure a maximum of THREE members of the IT Group's committee have flash drive copies of the membership data. Only the Chairman will have the right to edit this data.
7. Hold personal data for a maximum of TWO years after the member has ceased to attend classes regularly in order to keep them informed of new provision availability.
8. informed members that their data is available for inspection and may be requested by completing a appropriate form. An administrative fee of £5 shall be payable for this service.
9. ensure copies of this policy and the form required for 8. above shall be available on the IT Group's website (www.cwitgroup.btck.co.uk) or available on request.

Greg Herdman (revised 20 May 2014)