



General Data Protection Regulation (2018) Clarborough & Welham IT Group Policy

Within the following sections of this policy document Clarborough & Welham IT Group may be referred to as the 'Group' or 'IT Group'.

What is the GDPR?

The General Data Protection Regulation (GDPR) is a new set of European Union (EU) regulations due to come into force on 25th May, 2018. It will change how organisations process and handle data, with the key aim of giving greater protection and rights to individuals. The UK Government currently has a new Data Protection Bill passing through Parliament. This Act of Parliament will largely incorporate GDPR with a few small differences.

What data does Clarborough & Welham IT Group hold for individuals?

When individuals first enrol for classes, they complete an **Enrolment Form**. This asks for the following personal data: Surname, Forename(s), telephone number and e-mail address. No other data is either collected or recorded.

Reasons for holding personal data

Clarborough & Welham IT Group holds personal data for individuals attending classes:

- to contact them in the event of changes/cancellations of class session due to unforeseen circumstance such as bad weather, road accidents, etc.
- to provide personal out-of-class support such a lesson follow-ups or technical advice.
- to advise forthcoming class session times. Since experience shows many class members attend on a 'seasonal' basis, this will require personal data retention for up to 12 months.

What is new?

There are new and extended rights for individuals in relation to the personal data an organisation holds about them, for example, and extended right to access and a new right of data portability. You can obtain further information about these rights from the Information Commissioner's Office (ICO) at www.ico.org.uk or via their telephone helpline (0303 123 1113). In addition, organisations will have an obligation for better data management and a new regime of fines will be introduced for use when an organisation is found to be in breach of the GDPR.

What are the main principals of the GDPR?

The GDPR states that personal data held by the IT Group must be:

- processed lawfully, fairly and in a transparent manner.
- Collected only for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Held only for the absolute time necessary and no longer.
- Processed in a manner that ensures appropriate security of the personal data.

What is personal data?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data,

including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Can Group members ask for their data to be deleted?

Class members can ask for their personal data to be deleted. However, individuals should be aware that they would lose the services mentioned above (***Reasons for holding personal data***) should they so request.

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

- a) Appoint a member of the Group's committee as Data Protection Officer to manage all aspects of this policy.
- b) Periodically inform those from whom we have obtained data, that we hold it.
- c) Periodically ensure that our data is up-to-date.
- d) Ensure the data is only adequate for purpose – which in IT Group case means appropriate for emergency or other basic contact details.
- e) Keep data safe such that it cannot fall into third party hands.
- f) Determine which members of our committee should have access to the data and under
- g) what conditions (i.e. time frame, etc).
- h) Delete the data once it is no longer relevant.
- i) Have mechanism in place for members to review their data.

To these ends, the IT Group will...

1. Designate the Chairperson as Data Protection Officer.
2. 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.
3. Not pass any personal data to any third party unless required to by law.
4. Regularly check with members that their data has not changed since the last check.
5. Only enter data comprising **name, telephone number** (including **mobile** if appropriate) and **e-mail address**) into a spreadsheet for the above purposes.
6. Store 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).
7. Only the Data Protection Officer will have the right to view or edit this data.
8. Hold personal data for a maximum of 12 months after the member has ceased to attend classes regularly in order to keep them informed of new provision availability.
9. Inform members that their data is available for inspection and may be requested by completing an appropriate form. An administrative fee of £5 shall be payable for this service.
10. 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.

Draft policy (2) dated 27 April, 2018
G.A.Herdman
Chairman, Clarborough & Welham IT Group