

## 1. Data protection principles

Forth Valley Orienteers (FVO) is committed to processing data in accordance with its responsibilities under the General Data Protection Regulations (GDPR).

Article 5 of the GDPR requires that personal data shall be:

- a. Processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

## 2. General provisions

- a. This policy applies to all personal data processed by FVO;
- b. FVO is [exempt from registering](#) with the Information Commissioner’s Office (ICO) as an organisation that processes personal data;
- c. FVO is not required [by the regulations](#) to appoint a data protection officer, and we have chosen not to do so. However, we have appointed our club secretary to be the "Responsible Person" for overseeing our compliance with data protection;
- d. All our members and volunteers are responsible for data protection. Everyone has their role to play to ensure that we remain compliant with data protection laws. Detailed practical steps that members and volunteers should follow are listed in section 10 of this policy.

### **3. Lawful, fair and transparent processing**

- a. To help ensure its processing of data is lawful, fair and transparent, FVO shall maintain a register of all systems or contexts in which personal data is processed by FVO (the "Register of Systems");
- b. Individuals have the right to access their personal data and any such requests made to FVO shall be dealt with timeously.

### **4. Lawful purposes**

- a. All data processed by FVO must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see [ICO guidance](#) for more information);
- b. FVO shall note the appropriate lawful basis in the Register of Systems;
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data;
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in FVO's systems.

### **5. Data minimisation**

FVO shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

### **6. Accuracy**

FVO shall take reasonable steps to ensure personal data is accurate and kept up to date.

### **7. Archiving / removal**

FVO shall archive and remove data as shown in FVO's data privacy statement and as detailed below in section 10.

### **8. Security**

- a. FVO shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. Access to personal data shall be limited to members who need access to data.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable.
- d. Appropriate back-up and disaster recovery solutions shall be in place.

## 9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, FVO shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the [ICO website](#))

## 10. Practical Day to Day steps for members and volunteers

- a. Treat all personal data with respect and how you would want your own personal data to be treated;
- b. Immediately notify the Responsible Person if you become aware of or suspect the loss of any personal data or any item containing personal data;
- c. Files containing personal data which are held on laptops, mobile devices or removable storage devices (such as usb sticks) should be password protected and/or encrypted;
- d. If you email a file containing personal data it should be encrypted or password protected. The decryption key or password should be forwarded separately from the email;
- e. Files containing personal data should be securely removed from laptops or removable storage devices which are borrowed (to enable FVO to put on an orienteering event) before the laptops or storage devices are returned;
- f. If you are responsible for maintaining a set of personal data for FVO, then you should ensure that old data is removed in the timescales set out in FVO's Data Privacy Notice. In particular;
  - membership data shall be securely deleted four years after a member leaves the club;
  - electronic entry data, paper entry forms and accident forms shall be securely deleted four years after the event; and
  - web server logs containing personal information should be removed after three months.
- e. If the Responsible Person receives a subject access request, the Responsible Person shall promptly ask each of the people responsible for maintaining the different sets of personal data to timeously gather the required information, so that FVO can respond to the request.
- f. The Responsible Person may receive requests to correct or delete personal data. If the request is in respect of correction then person responsible for maintaining the data set should ensure the correction of the data. If the request is in respect of deletion, then FVO should discuss the request and delete the data if it is appropriate to do so.
- g. If you hold an extract of a set of personal data; then you should ensure that old copies of such data extracts are securely deleted if you are provided with an updated set of

personal data. You should also ensure that you securely delete such data extracts if you no longer need to process them on behalf of FVO.

- h. Do not transfer personal data outside the European Economic Area (EEA) unless such transfer is in compliance with our Data Privacy Statement. In particular, this affects both:
  - cloud storage of data; and
  - The use of cloud e-services. If you have a need to use such a service, notify the Responsible Officer so that FVO can consider and amend its Data Privacy Policy appropriately.
- i. If you are the organiser for an event, then you should ensure that:
  - the latest versions of the club's entry forms which are held on the FVO's website are used;
  - paper entry forms should be sent to the membership secretary after the event;
  - online entry data containing participants contact details (in an unencrypted, non-password protected comma separated values file format) should be uploaded to the secure storage area of club website after the event, and local copies securely deleted; and
  - any accident forms are also lodged with the membership secretary.
- j. If you become aware of a club use of personal data which is not described in the Register of Systems or in the club Data Privacy Notice, or become aware of a new usage of personal data which is needed for the club to undertake its activities, the please promptly notify the Responsible Officer.