

# Data Protection Policy, February 2020

## Introduction

As part of its activities Woodcraft Folk makes use of personal information about its members, employees, volunteers, donors, customers and others.

Woodcraft Folk recognises the importance of using personal and sensitive data in an appropriate way and protecting the person information which it, and complying with data protection law in doing so.

This policy sets out Woodcraft Folk's approach to protecting data, and provides guidance to members, staff and volunteers on how to deal with any personal or sensitive information they handle as part of their roles.

## Contents

### **1. Legal Framework / Data Protection Principles**

- 1.1 Relevant law & regulations
- 1.2 Key definitions
- 1.3 Data Protection Principles
- 1.4 Lawful bases for processing data
- 1.5 Individual Rights
- 1.6 Registration with ICO
- 1.7 Application of the policy

### **2 Whose data do we hold and why**

- 2.1 Categories
- 2.2 Privacy Notices / Privacy Policy
- 2.3 Data Retention policy
- 2.4 Third parties

### **3. Procedures and accountability**

- 3.1 Data Controller
- 3.2 Data Processors
- 3.3 Procedure for Subject Access Requests
- 3.4 Questions or Complaints

### **4. Policy Review**

# 1. Legal Framework & Data Protection Principles

## 1.1 Relevant law & regulation

The General Data Protection Regulation (GDPR) is an EU-level agreement that is incorporated into UK law by the Data Protection Bill 2017, which updates the existing Data Protection Act (1998). The Regulations comes into effect on 25 May 2018. The most significant change is to clarify the lawful bases on which data can be processed (particularly in relation to consent), a much stronger requirement to demonstrate compliance and much more severe punishment for failure to comply.

The Privacy & Electronic Communications Regulations (PECR) covers all electronic communication, e.g. emails, social media, video calling, phone systems using VOIP (Voice Over Internet Protocol), cookies on websites, etc. The 2003 regulations are being updated to bring them into line with GDPR.

## 1.2 Key Definitions

The Data Protection Principles apply to Personal Data and to Special Categories of Personal Data (Sensitive Personal Data under the 1998 Act).

**Personal Data** means 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.

Data protection legislation applies to both automated (digital) personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the legislation depending on how difficult it is to attribute the pseudonym to a particular individual.

**Special Categories of Personal Data** are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data used for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Higher standards are in place in relation to the processing of Special Categories of Personal Data. For Woodcraft Folk purposes, explicit consent would usually be required for the processing of Special Categories of Personal Data. The main exception might be data concerning health, where it may be in the vital interests of a young person that we process data relating to their health and they are unable to give consent, but this would only apply in exceptional circumstances. Normally explicit consent should be gained in advance from the young person (or their parent / guardian depending on their age).

**Processing data** includes gathering, storing, updating, making use of, deleting or archiving.

A **Data Controller** determines the purposes and means of processing personal data. The controller shall be responsible for, and be able to demonstrate, compliance with the principles. The Data Controller for Woodcraft Folk is the General Secretary (Director of Operations & Finance from September 2018).

A **Data Processor** is responsible for processing personal data on behalf of a controller. In Woodcraft Folk, Data Processors include staff, volunteers and third parties.

### 1.3 Data Protection Principles

There are six Data Protection Principles:

Personal Data must be:

1. processed **lawfully, fairly and in a transparent manner** in relation to individuals;
2. 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;
3. **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed;
4. **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;
5. 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
6. 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.

### 1.4 Lawful bases for processing personal data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- (a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) **Vital interests**: the processing is necessary to protect someone's life.
- (e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the

individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If you are processing **special category data**, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

If you are processing **data about criminal convictions**, criminal offences or related security measures, you need both a lawful basis for processing and a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for processing and your criminal offence data condition so that you can demonstrate compliance and accountability.

## 1.5 Individual Rights

The legislation sets out eight areas where an individual has rights relating to their personal data.

1. The **right to be informed**. We must tell them what data you are processing and why – this is done through a privacy statement or fair usage notice.
2. The **right of access**. An individual can make a Subject Access Request, following which we must, for no charge, supply a copy of any data we hold about them within one month of receiving the request.
3. The **right to rectification**. We must correct any inaccuracies in the information that they inform us about.
4. The **right to erasure**. Also known as the "right to be forgotten", this is slightly misleading as we may be required to keep some data for legal reasons even if the individual does not want us to contact them in future.
5. The **right to restrict processing**. An individual can put constraints on the use of the data they provide – again this may be over-ridden by legal requirements.
6. The **right to data portability**. More relevant in a commercial setting, but we must ensure that the data is held in a format that could be transferred to an alternative provider if the individual wishes.
7. The **right to object**. We must have in place a complaints procedure.
8. **Rights in relation to automated decision making and profiling**. If we make decisions or take action based on the analysis of their data using algorithms or other automated processes, they can insist that it is looked at again by a human.

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

## 1.6 Registration with Information Commissioner's Office (ICO)

As a registered charity, Woodcraft Folk is registered with the ICO as a Tier 1 organisation (small business or charity). The annual renewal falls due in January.

## 1.7 Application of the policy

This policy applies to the entire Woodcraft Folk organisation, all groups, centres, projects, regions, Nations and decision-making bodies.

All Woodcraft Folk staff should be aware of this policy, and are responsible for complying with it when dealing with personal data as part of their job.

Woodcraft Folk will provide training and guidance on this policy and on data protection to those staff who regularly deal with personal data as part of their jobs.

All Woodcraft Folk groups, when they process personal data relating to their group members or volunteers, they do so on behalf of Woodcraft Folk and therefore must comply with this policy. Specific guidance is available for groups and centres which will help them process data consistently.

Any questions regarding this policy, or its practical implementation, should be raised with the Woodcraft Folk Data Controller ([data@woodcraft.org.uk](mailto:data@woodcraft.org.uk)).

## **2. Whose data do we hold and why**

### **2.1 Categories**

Woodcraft Folk holds personal data on individuals in the following categories:

1. Beneficiaries
  - a. Beneficiaries under the age of 13
  - b. Beneficiaries aged 13 or over
2. Parents / Guardians of Beneficiaries
3. Enquirers (potential, volunteers, beneficiaries, etc.)
4. Members / Volunteers working with children and young people
5. Members / Supporters / Donors not working with children and young people
6. Branch Officers
7. Trustees
8. Staff and contractors
9. Job applicants
10. Customers
11. Centre Guests
12. Visitors at our events, including international delegations.

In all cases Woodcraft Folk may hold information about people currently in one of these categories or people who have previously been in one of these groups. The basis for holding this data is set out in the Privacy Notice for each categories.

### **2.2 Privacy Notices**

The Privacy Notices form part of Woodcraft Folk's Privacy Policy and can be found at: <https://woodcraft.org.uk/privacy>

## 2.3 Data Retention Policy

Data is retained for the following lengths of time:

<b>Category of data</b>	<b>Retention Period</b>
Members / Beneficiaries	while in membership
Former Members / Beneficiaries	three years from end of membership
Parents / Guardians of Beneficiaries	while beneficiary is in membership
Parents / Guardians of former Beneficiaries	three years from end of beneficiary's membership
Donors / Supporters	seven years from most recent donation
Former Donors / Supporters	seven years from most recent donation
Customers / Guests (Folk Supply, Centres) and Former Customers / Guests	three years from most recent custom
Job applications	6 months
Data relating to current employees	while employed
Data relation to former employees	six years from leaving date
Data relating to safeguarding incidents or which may be legally required in relation for future safeguarding incidents	indefinite

Anonymised, aggregated data, or data that is already in the public domain may be added to our private or public archive for research purposes.

Personal data that we are required to keep to meet audit, legal, safeguarding or other regulatory requirements will be kept in our restricted archive, which can only be accessed by individuals authorised by General Council in line with the data protection procedures (see section 3, below).

## 2.4 Third parties

Woodcraft Folk does not sell personal data. Woodcraft Folk only shares personal data with third parties where this is necessary to provide services to individuals in one or more of the categories set out in 2.1 (above).

The following, non-exhaustive, list includes the main examples of the type of third party with which Woodcraft Folk may share personal data. In all instances, Woodcraft Folk seeks assurances from the third party that their data protection policy and procedures comply with legal requirements and Woodcraft Folk policy and procedures where appropriate.

### **Third Parties who may process personal data on behalf of Woodcraft Folk:**

- Database provider – in order to manage individual and branch membership, contact with individuals and officers of branches, online payments, we contract with a database provider.

- Website provider – in order to enable members only access and to customise your experience using our website, we maintain a database of website users which our website provider manages in line with our instruction.
- Event management software provider – in order to enable members to sign up to and pay for activities we contract with a group/event management software provider
- Centre bookings software provider – to facilitate efficient online bookings of our residential centres we contract a campsite/venue bookings software provider
- Online shop provider – in order to offer Folk Supply online, we contract with an online shopping provider.
- Email provider – in order to manage our email we contract with an email provider.
- HR support supplier – in order to manage our HR function, we contract with a provider of employment law advice and staff management tools.
- Payroll supplier – in order to manage our payroll, we contract with a payroll provider.
- Pension Provider – in order to comply with pensions legislation, we contract with a pension provider for our staff.
- IT support provider – in order to ensure the maintenance and security of our IT, we contract with an IT support provider.
- Online Payment processor – in order to offer online payment facilities, we contract with an online payment processor.
- Safeguarding authorities – in order to ensure the safety of children and young people and to comply with legislation, we may pass personal information to Local Authorities Designated Officers, the Police, the Courts, the Disclosure and Barring Service (England & Wales), the Protection of Vulnerable Groups service (Scotland) and other agencies as required.
- Activity Providers – in order to ensure the safety of our beneficiaries, volunteers, guests and customers, we may share personal data with activity providers.
- Accommodation / Venue providers – in order to ensure the safety of our beneficiaries, volunteers, guests and customers, we may share personal data with providers of venues and/or accommodation.

### **Third Parties who do not process personal data on behalf of Woodcraft Folk:**

- Online DBS check provider - no personal data is passed from Woodcraft Folk to GBG, members create their own account with GBG and any data shared is covered by GBG policies.
- Event and group online management software provider – no personal data is passed from Woodcraft Folk to Groop, members and participants create their own account with Groop and any data shared is covered by Groop policies. Woodcraft Folk then uses the data supplied to Groop to ensure the safe and positive engagement of individuals in our activities and events.
- Centre booking online management software provider – no personal data is passed from Woodcraft Folk to Gemapark. Centre guests enter their data on to Gemapark's secure platform to make availability enquiries, bookings and payments. Woodcraft Folk then uses the data supplied to Gemapark to effectively manage group bookings.
- Direct Debit processor – Members setting up Direct Debits with Woodcraft Folk enter their details on our Direct Debit provider's website. They share personal data with

Woodcraft Folk to enable us to ensure that payments are linked to the correct individual in our systems.

- Social Media platforms – Members using social media, e.g. Facebook groups, do so under the Facebook data protection and privacy policies.

## **3. Data Processing Procedures and Accountability**

### **3.1 Data Controller**

The General Secretary (Director of Operations & Finance from September 2018) is the Data Controller for Woodcraft Folk. Woodcraft Folk does not meet the threshold to require a Data Protection Officer as set out in the Act (i.e. our core activities do not involve the large scale processing of special categories of personal data or data relating to criminal convictions and offences).

In addition to the statutory duties of a Data Controller (A controller determines the purposes and means of processing personal data.), the General Secretary (Director of Operations & Finance from September 2018) is responsible for ensuring that:

- This policy is up to date
- Woodcraft Folk's registration with the ICO is up to date
- Appropriate advice is given to members, volunteers and staff
- Requests and complaints relating to data are responded to promptly
- Providing a report to Trustees at least twice per year highlighting emerging best practice, any breaches of the policy and how they were dealt with
- Lessons learnt and good practice is shared throughout the organisation

### **3.2 Data Processors**

There are multiple Data Processors in Woodcraft Folk. A processor is responsible for processing personal data on behalf of a controller. These include:

- Staff
- Volunteers
- Third Parties

### **3.3 Procedure for Subject Access Requests**

Subject Access Requests should, where possible be submitted to the Data Controller by email [data@woodcraft.org.uk](mailto:data@woodcraft.org.uk). We recognise that Subject Access Request may be made in other formats or to data processors rather than to the Data Controller.

Where a Subject Access Request is made to a Data Processor, the request should be passed to the Data Controller by email within three days to ensure that Woodcraft Folk can respond appropriately within the one month time limit set down in law.

### **3.4 Questions or Complaints**

If you have questions about how we use your data that are not answered by our Privacy Policy (<https://woodcraft.org.uk/privacy>), please email [data@woodcraft.org.uk](mailto:data@woodcraft.org.uk).

If you have a complaint about how we have used your data, please contact [data@woodcraft.org.uk](mailto:data@woodcraft.org.uk). If you are unhappy with our response to your complaint, you can escalate your complaint to the Information Commissioner's Office: <https://ico.org.uk/concerns/>.

## **4. Policy Review**

This policy was original agreed by General Council on 21 April 2018.

This policy was reviewed in October 2019 and was presented for approval to General Council in November 2019.