08. Data Protection and Confidentiality Policy

0. Background

This policy is based on guidance on the Information Commissioner's Office (ICO) website (https://ico.org.uk/) document "guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf" V 1.0.751 dated 22 May 2019.

The General Data Protection Regulation (GDPR)

The GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- can be indirectly identified from that information in combination with other information.
- personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

Woking Strokeability is a personal data Controller

Under GDPR, Woking Strokeability is a personal data "Controller". We exercise overall control over the purposes and means of the processing of personal data. As a Controller we must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements.

GDPR Data Protection Principles

1. **Lawfulness, fairness and transparency.** Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. **Purpose limitation**. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data minimisation**. Personal data must be adequate, relevant and limited to what is necessary.
4. **Accuracy**. All reasonable steps must be taken to ensure personal data is not incorrect or misleading as to any matter of fact. If personal data is incorrect or misleading, reasonable steps must be taken to correct or erase it as soon as possible.
5. **Storage limitation**. Data must be kept in a form which permits identification of data subjects for no longer than is necessary.
6. **Accountability.** The Management Committee and Trustees are responsible for complying with the UK GDPR and must be able to demonstrate compliance.
7. **Integrity and confidentiality (security**). Personal data must be processed securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

Data Protection Fee

A registration self-assessment was carried out on the Information Commissioner's Office (ICO) website https://ico.org.uk/. The assessment indicated that Woking Strokeability is a not-for-profit organisation that qualifies for an exemption from the data protection fee. Woking Strokeability:

- only process information necessary to establish or maintain membership or support;
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- only hold information about individuals whose data we need to process for this exempt purpose; and
- the personal data we process is restricted to personal information that is necessary for this exempt purpose.

It is noted that Woking Strokeability need to adhere to the principles of the General Data Protection Regulations and understand best practice for managing information.

Data Protection Officer (DPO)

Woking Strokeability does not need to appoint a DPO. The ICO web site states that "a small organisation is unlikely to need a data protection officer (DPO)". Woking Strokeability would only need to appoint a DPO if:

- our core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- our core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

The Secretary has responsibility for data protection. The Secretary looks after the privacy notice, keeps membership records up-to-date and will, in the first instance, deal with any data protection requests.

The Secretary is responsible for briefing the Trustees and Management Committee on the importance of data protection and the need for it be considered at all stages of information collection, use and storage, and also to provide some simple, practical advice and guidance that can be taken by all.

The Trustees and Management Committee have the responsibility to help:

- Identify and continuously review areas that could cause problems.
- Define and deploy processes and procedures that will maintain confidentiality.

Lawful Basis Assessment

The lawful basis assessment tool on the ICO website indicated that CONTRACT is likely to be an appropriate lawful basis. Suggested actions are:

- When processing special category data or criminal offence data, Woking Strokeability need to identify a separate condition to allow the processing of this type of data.
    - The Woking Strokeability statement is attached as Appendix 1.
- Woking Strokeability need to demonstrate how and why processing is necessary for the contract. Ensure that this decision is documented, and include information about purposes and lawful basis in the privacy notice.
    - The Woking Strokeability Data Privacy Notice attached as Appendix 2.

1. Lawfulness, fairness and transparency

The lawful basis for Woking Strokeability collecting and using personal, private data is contract. This data is used to keep contact with members & carers and maintain a membership register.

- Information on data privacy is provided through our application form and the "Data Privacy Notice" available on our website or through a Trustee or member of the Management Committee.
- Personal data is provided by an applicant and/or their carer directly on the membership form. All members have confirmed their consent to Woking Strokeability retaining and processing their private data either by signature or email. The form states - "I consent to Woking Strokeability processing my personal data and am aware that my consent can be withdrawn at any time."
- Personal data held is only that information required to run the club
    - Member registration forms and member contact lists. These are stored as pdf files on our SharePoint intranet site.
    - Email addresses are also held on the servers of our website, www.wokingstrokeability.com, to facilitate the circulation of general communications to all members.

Members have individual rights which are responded to in the context of Woking Strokeability as listed below:

- *the right to be informed;*
    - By consent statement on application form for new members: "I consent to Woking Strokeability processing my personal data and am aware that my consent can be withdrawn at any time"
    - By a Data Privacy Notice on our website.
    - By communication to all members providing information on changes to our Data Privacy Notice when it is updated.
- *the right of access;*
    - A member can access their data at any time by consulting the membership list or requesting a copy from the Secretary, member of the Management Committee or Trustee.
- *the right to rectification;*
    - Personal details can be updated at any time by members advising the Secretary, member of the Management Committee or Trustee..
- *the right to erasure;*
    - Membership details can be erased at any time at the request of a member or their carer. This will result in their membership form, email address and entry on the membership contact register being deleted and the member leaving Woking Strokeability.
- *the right to restrict processing;*
    - Members can remove their consent to Woking Strokeability processing their data at any time, however this may result in the suspension of the member.
- *the right to data portability;*
    - Details held by Woking Strokeability will be provided as a PDF of the application form and an image of the individual's entry in the membership contact register.

- *the right to object;*
    - A member can object to use of their data at any time. If this results in the useable data being less than the minimum required it will result in the member being suspended.
    - The minimum data required for remaining a member is name, address and an email address or contact phone number. Ideally we prefer both an email address and a phone number.
- *the right not to be subject to automated decision-making including profiling*
    - Not applicable, Woking Strokeability do not use automated data processing.

Woking Strokeability is committed to maintaining high standards of confidentiality in all aspects of its work. This includes records and information pertaining to members, their carers and volunteers.

- In cases where there are concerns relating to the safeguarding of members Woking Strokeability's Safeguarding Policy will apply.
- In all but specific circumstances (e.g. serious complaints), the decision as to who should be given of a piece of confidential information outside of the scope of information identified in this document is the member, carer or volunteer to whom it applies. Where such consent is sought it is necessary to tell the member, carer or volunteer why there is a need to disclose information and to whom. Once consent has been obtained, it is the responsibility of the person passing on any information to ensure that this is only done on the terms agreed.
- No member, their carer or volunteer has the right to view any other party's personal data except as specifically provided for in this policy.

Data Breaches

- Our approach to data handling is such that we do not believe that any breech is likely to result in a risk to the rights and freedoms of individuals.
- If a breach occurs the Secretary, another member of the Management Committee, a Trustee, or a DPO will be invited by the Management Committee or Trustees to investigate the breech and where necessary make such changes to data access and processes, and report as may be required.

Subject access requests

- Woking Strokeability will respond to any subject access request and do not expect to have to charge.

2. Purpose Limitation

Woking Strokeability collect personal data through completed application forms to create membership contact lists & email circulation lists, and be aware of conditions that could lead to a members sudden loss of consciousness.

Hard copy membership forms are scanned, deleted and stored electronically for reference.

- Information on conditions that could lead to a sudden loss of consciousness is shared with the Management Committee, Trustees and Instructors.
- Names, member contact data and emergency contact data is shared with the Management Committee and can be shared with members of the club.
- No data is shared with third parties.

3. Data Minimisation

The minimum data required for remaining a member is name, address and an email address or contact phone number. Ideally we prefer both an email address and a phone number.

- A member can object to use of their data at any time. If this results in the useable data being less than the minimum required it will result in the member being suspended.
    - If after suspension a member would like to return consent to Woking Strokeability they will be requested to complete a current application form to confirm contact details and consent.
- Membership details can be erased at any time at the request of a member or their carer.

Unless otherwise requested, personal data on members, carers and volunteers is held for up to 4 years after no longer attending any meeting or social event held by the group.

- Data is normally cleansed after the AGM each year by the Secretary.

4. Accuracy

Personal details can be updated at any time by members advising the Secretary, a member of the Management Committee or a Trustee.

- If any member of the Management Committee or a Trustee identifies that the data referring to any member is incorrect they should take steps to ensure that the correct data is identified and records updated accordingly.

5. Storage Limitation

Unless otherwise requested, data on members, including membership forms, carers and volunteers is held for up to 4 years after no longer attending any meeting or social event held by the group.

Data is held in the Woking Strokeability SharePoint site and on the servers of our web site provider.

- Data on the servers of our web site provider consists of member email addresses which are deleted when a member is removed from either our email list of active members or the email list of those interested our updates. This can be by request or after the annual review of active / interested members each year.
- Data held in the SharePoint site is cleansed after the AGM each year by the Secretary. This will consist of deleting relevant application forms and membership contact lists more than 3 years old at the end of Woking Strokeability's year. For example, membership contact lists stored on the intranet site dated before 1 November 2017 should be deleted in the first three months of year 2020-21, i.e. before 31 January 2021.

6. Accountability

The Management Committee and Trustees are accountable for all personal data relating to members, their carers and volunteers.

All members in possession of confidential information should:

- Make sure any discussion relating to information of another, takes place in an appropriate venue, e.g. not in a place where others, who are not entitled to know, can hear about it.
- Not gossip about other members their carers or volunteers.
- Not leave confidential information lying around.

- Not write anything derogatory about other members their carers or volunteers in a file, email, on social media or anywhere else.

Breaches of confidentiality by members, their carers or volunteers will normally be treated within the remit of Woking Strokeability Complaints Policy.

7. Integrity and confidentiality (security)

Data held on our web site host's server:

- A link to privacy policy of the organisation who host our website, Kualo, is provided on our web site www.wokingstrokeability.com.
- To protect members personal email addresses, mails to all members on our 'active' and 'interested' email circulation lists are sent via an alias, e.g. 'active@wokingstrokeability.com'.
- Members of our Management Committee and all Trustees are given their own individual Woking Strokeability email address. For example the Secretary can use the addresses 'secretary@wokingstrokeability.com' or 'ben@wokingstrokeability.com' both of which will forward on to a personal email address.
- Kualo regularly back up the data held on our behalf on their servers.

Data held on the Woking Strokeability Microsoft Office 365 SharePoint intranet site.

- The intranet site holds all of the records Woking Strokeability need to manage the charity. This includes pdf copies of membership forms and membership contact lists.
- Our account is primarily used to manage and store documents in a variety formats, e.g. MS Word, Excel, PowerPoint, PDF, Zip, MP4 etc., in a defined high-level file structure.
    - 00. Blank Forms
      01. Policies and Related Documents
      02. Membership & Contacts
      03. Social
      04. Meetings & Current Actions
      05. Finance
      06. Guidance, Seminars & Reports
      07. Charity Commission
      08. Insurance
      09. Associated Organisations
      10. Correspondence & General
      11. Marketing & Fundraising
      12. Accident Reports
      13. Software- Website, 0365, Social Media
- Microsoft is responsible for ensuring high availability and disaster recovery for Office 365 SharePoint. Gartner stated that "Microsoft O365 offers robust disaster recovery, but limited native backup and recovery".
    - To provide a more easily accessible backup Woking Strokeability carry out a manually driven process using zip files to store data on a separate service.
    - The current process is to view data in OneDrive, select file view, then download the complete structure of all 14 high-level folders as zip files. This allows a restore of all files in the current structure to SharePoint/OneDrive or any other cloud storage service e.g. Dropbox, Box, pcloud, Google Drive etc.
    - Woking Strokeability backups are stored in the cloud on the pcloud service. The account is managed by the Secretary. The account password is given to all members on the Management Committee and Trustees

      Login: 'secretary@wokingstrokeability.com'

      url: https://www.pcloud.com/eu

- The Secretary is responsible for carrying out backups on a regular basis and advising the Management Committee and Trustees.

Data is also held on paper and in members individual electronic devices such as laptops, tablets and phones.

- Personal data on the membership contact list in PDF or paper format is freely available to members.
  - The list contains the following statement in red … "CONFIDENTIAL - PRIVATE INFORMATION DO NOT CIRCULATE OUTSIDE OF WOKING STROKEABILITY"
- The Secretary is responsible making all members aware of the need for data security and providing relevant advice.
  - All members of the Management Committee and Trustees have access to the complete set of Woking Strokeability data. The Secretary has the responsibility of reminding them of the need to follow basic data security recommendations. See Appendix 3.
  - Woking Strokeability rely on email as the primary communication medium with the membership. The Secretary has the responsibility of reminding the membership simple data security guidelines. These will include keeping their operating system Microsoft Windows, macOS, Android or iOS up to date and making use of anti-virus and firewall software and strong passwords.

Dated: 18 January 2021

Appendix 1 – Special Category Data Statement

This appendix is based on the ICO document "appropriate-policy-document-1" template V1.0 dated 4 November 2019. Details reproduced directly from the policy document are in *italics* and indented , the Woking Strokeability response in plain text.

Introduction

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

This document should demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it should outline your retention policies with respect to this data. (See Schedule 1 Part 4).

If you process SC or CO data for a number of different purposes you do not need a separate policy document for each condition or processing activity – one document can cover them all. You may reference policies and procedures which are relevant to all the identified processing. Whilst you may explain your compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, you should provide the data subject with sufficient information to understand how you are processing their SC or CO data and how long you will retain it for.

However if you rely on one of these conditions, your general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;

(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and

(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

The APD therefore complements your general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge.

Description of data processed

Give a brief description of each category of SC/CO data processed. You may wish to refer to your Article 30 record of processing for that particular data:

Statement on Data Privacy Notice

- Woking Strokeability collect special category data through the application form to be aware of conditions that could lead to a sudden loss of consciousness. This information is only shared with the Management Committee and instructors.

Schedule 1 condition for processing

Give the name and paragraph number of your relevant Schedule 1 condition(s) for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

Statement on Data Privacy Notice

- Woking Strokeability collect special category data through the application form to be aware of conditions that could lead to a sudden loss of consciousness. This information is only shared with the Management Committee and instructors.

Procedures for ensuring compliance with the principles

You need to explain, in brief and with reference to the conditions relied upon, how your procedures ensure your compliance with the principles below.

This helps you meet your accountability obligations. You have a responsibility to demonstrate that your policies and procedures ensure your compliance with the wider requirements of the GDPR and in particular the principles. The sensitivity of SC and CO data means the technical and organisational measures you have in place to protect such data are crucially important.

The questions listed in each box are intended to help you describe how you satisfy each principle generally, and are based on the checklist for each principle provided in the Guide to the GDPR. They are not exhaustive and are only intended to act as a guideline.

In explaining your compliance with the principles you should consider the specifics of your processing with respect to the SC and CO data you have identified above.

You may also wish to answer other questions which are included in our Guide to the GDPR checklists (see links in each section below).

There is also no requirement to reproduce information which is recorded elsewhere – questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.

Accountability principle

i. Do we maintain appropriate documentation of our processing activities?

ii. Do we have appropriate data protection policies?

iii. Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?

Statement on Data Privacy Notice

- Woking Strokeability collect special category data through the application form to be aware of conditions that could lead to a sudden loss of consciousness. This information is only shared with the Management Committee and instructors.

Principle (a): lawfulness, fairness and transparency

i. Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data?

ii. Do we make appropriate privacy information available with respect to the SC/CO data?

iii. Are we open and honest when we collect the SC/CO data and do we ensure we do not deceive or mislead people about its use?

See response to accountability principle above

Principle (b): purpose limitation

i. Have we clearly identified our purpose(s) for processing the SC/CO data?

ii. Have we included appropriate details of these purposes in our privacy information for individuals?

iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?.

See response to accountability principle above

Principle (c): data minimisation

i. Are we satisfied that we only collect SC/CO personal data we actually need for our specified purposes?

ii. Are we satisfied that we have sufficient SC/CO data to properly fulfil those purposes?

iii. Do we periodically review this particular SC/CO data, and delete anything we don't need?.

Woking Strokeability are satisfied that we only have the SC data we need and that it is periodically reviewed for deletion.

Principle (d): accuracy

i. Do we have appropriate processes in place to check the accuracy of the SC/CO data we collect, and do we record the source of that data?

ii. Do we have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and do we update it as necessary?

iii. Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?

Woking Strokeability are satisfied that sufficient processes in place to maintain data accuracy.

Principle (e): storage limitation

i. *Do we carefully consider how long we keep the SC/CO data and can we justify this amount of time?*

ii. Do we regularly review our information and erase or anonymise this SC/CO data when we no longer need it?

iii. Have we clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?

Woking Strokeability are satisfied that sufficient processes in place to limit data storage.

Principle (f): integrity and confidentiality (security)

i. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?

ii. Do we have an information security policy (or equivalent) regarding this SC/CO data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?

iii. Have we put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing?

SC data is only stored on PDF application forms and is not used in any other documentation. Woking Strokeability are satisfied that sufficient processes in place to maintain integrity and confidentiality.

Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of SC/CO data (this could include a link to your retention policy if you have one). You need to explicitly indicate how long you are likely to retain each specific category of SC/CO data.

Statement on Data Privacy Notice

- Unless otherwise requested, data on members, carers and volunteers can be held for up to 4 years after no longer attending any meeting or social event by the group. The Secretary cleanses data after the AGM each year.

APD review date

This Appropriate Policy Document is due for review within 24 months of its issue date.

Appendix 2 – Data Privacy Notice 2021

Woking Strokeability uses private personal data to keep contact with members and carers and maintain a register of members. An application form providing consent for Woking Strokeability to process personal data needs to be completed to become a member. Forms in hard copy are scanned and stored for reference and the hard copy securely destroyed. The lawful basis for Woking Strokeability processing private personal data is contract with the data subject.

Woking Strokeability collect special category data through the application form to be aware of conditions that could lead to a sudden loss of consciousness. This information is only shared with the Trustees, Management Committee and instructors.

Contact data is shared with members of the club and instructors but not third parties.

Any person joining Woking Strokeability except in the role of a carer or volunteer should understand that it implies that they are stroke survivor.

Unless otherwise requested, data on members, carers and volunteers can be held for up to 4 years after no longer attending any meeting or social event by the group. The Secretary cleanses data after the AGM each year.

- A member can access their details at any time by consulting the membership list or advising the Secretary or member of the Management Committee.
- The printed membership list contains the following statement in red … "CONFIDENTIAL - PRIVATE INFORMATION DO NOT CIRCULATE OUTSIDE OF WOKING STROKEABILITY
- The minimum data required for remaining a member is name, address and an email address or contact phone number. Ideally, we prefer both an email address and a phone number.
- Personal details can be updated at any time by a member advising the Secretary or member of the Management Committee.
- Members can remove their consent to Woking Strokeability processing their data (i.e. object to use of their data) at any time, however if this results in their data being less than the minimum required it will result in the member being suspended.
    - If after suspension, a member would like to return consent they will need to complete an application form to confirm their contact details and consent.
- Membership details can be erased at any time at the request of a member or their carer. This will result in the data being deleted and the member leaving Woking Strokeability.
- If you have a concern about the way Woking Strokeability is handling your information we will take your concern seriously and work with you to try to resolve it. If we cannot resolve your concern, you have the right to contact the Information Commissioner's Office (ICO).

Appendix 3 – Advice on Data Security

Cyberattacks don't only happen to large corporations. Small businesses, groups and charities have to protect their IT systems, too. Here are some practical steps based on recommendations by the ICO that can be taken today to tighten up data security.

1. Back up your data

Create a back-up copy of your data, and do this regularly. That way, if there's a virus attack, break-in, fire or flood, you don't lose everything. If using an external device as your back-up, you should encrypt it. It's also a good idea to store it in a lockable cupboard if you can.

2. Use strong passwords

Make sure you and anyone else involved uses strong passwords - including smartphones, laptops, tablets, email accounts and computers.

3. Be wary of suspicious emails

Educate yourself on how to spot suspicious emails. Checking for obvious signs such as bad grammar, requests for you to act urgently, and requests for payment will help you avoid being caught out. If it looks suspicious, don't trust it – and warn others not to either.

4. Install the current operating system and use anti-virus and malware protection

And keep them up-to-date. The National Cyber Security Centre has some useful advice and guidance on cyber security that can be obtained from the Secretary.

5. Don't leave paperwork or laptops etc. unattended

Data breaches can occur when paperwork, a laptop or any device is left unattended. This could be in the boot of a car, on a train, or at home. Make sure you take steps to protect the personal data you hold by being vigilant and storing it securely away when it's not in use.

6. Make sure your Wi-Fi is secure

Using unsecured home or public Wi-Fi connections could put personal data at risk, so you should make sure you always use a secure connection when connecting to the internet.

7. Lock your screen when you're away from your device

Take steps to lock your screen when you leave your device is a simple thing to do, but will prevent someone else from accessing your data.

9. Keep on top of who has access to what.

Only those having a good reason for accessing data should have the ability to do so.

10. Don't keep data for longer than you need it

Staying on top of what personal data you hold will save time and resources. It will also help with your data protection responsibilities. Only keep what you need, for as long as you need it.

11. Dispose of old IT equipment and records securely

Before you get rid of them, make sure no personal data is left on personal computers, laptops, smartphones or any other devices. The Secretary can provide advice such as using deletion software, or physical destruction of data storage devices. This will ensure no one can access information they're not supposed to see when you dispose of the equipment.