General Data Protection Regulations (GDPR) Policy

UKAFWSA has a requirement to process personal data in order to operate effectively. We will always do so lawfully, fairly and in a transparent manner. This policy describes our processes for doing so and is reflected in the privacy notice that is published on our website and included at Annex A. Our processes have been developed using the guidance provided by the UK Information Commissioner's Office (ICO).

Scope. This policy refers to our policy for processing personal data in the UK and EU, although information may be stored using cloud services that operate beyond the EU.

Data Controller. The Board of Trustees has appointed the Secretary as the Data Controller. He may be contacted at [insert email address]. Unless otherwise specified, it is the Data Controller's responsibility to manage the protection of personal data for the company. The Data Controller will routinely report to the Board of Trustees and will immediately inform them should it be suspected that data has been breached or that there has been any other non-compliance with company policy or the law. The Data Controller will maintain the appropriate documentation, of which this policy is a part, and oversee the maintenance of documentation by Data Processors.

Data Processors. Data Processors are responsible for processing personal data on behalf of the Data Controller. In practical terms, the principal Data Processor is also the Secretary, although most of the processing will be by the officers of the charity.

Data Processing Officer (DPO). The Board of Trustees has considered the appointment of a DPO and has determined that the nature of the company and the data which is processed does not demand such a role. However, the broad responsibilities and position of the DPO is to be adopted by the Data Controller.

Comment [RH1]: ICO guidance: Under the GDPR, you **must** appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

If you decide that you don't need to appoint a DPO, either voluntarily or because you don't meet the above criteria, it's a good idea to record this decision to help demonstrate compliance with the accountability principle.

Lawful Basis. The lawful basis on which UKAFWSA processes personal data is that we have a legitimate interest to do so. As an Armed Forces' sports charity this means that we need to do so in order to maintain effective linkages to representatives of our sponsors and donors ('points of contact'), including prospective sponsors and donors, and better match their needs with those of the charity. We also need to be able to maintain contact with our trustees, officers, volunteers, athletes, contractors, other charities and organisations, and members of the Armed Forces. We must be able to meet the requirements of the Charity Commissioners, HMRC or other government agencies. We do not believe that we can do this in a different way that is less intrusive and we believe that our sponsors, donors and others mentioned above would reasonably expect us to process personal information in this way.

Our Promise. UKAFWSA will take all reasonable steps to maintain the accuracy of our database of personal data. Where data is found to be inaccurate it will be rectified or erased without delay. We will only collect and store the data for the purposes consistent with the lawful basis described above. We will ensure 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. We do not anticipate a requirement to process the data for archiving purposes in the public interest, scientific, statistical or historical research purposes, although this may be allowable under the law.

Categories of Individuals and Personal Data. UKAFWSA has a requirement to process personal data in four broad categories:

> **Sponsors and Donors**. This category includes current, past and prospective sponsors and donors. These are the representatives of the companies who support the charity financially or in other ways. The personal data we process for clients includes their contact details such as phone numbers, email addresses, scans of their business cards and details of their support. It may include notes of discussions with them, including records of emails or other message formats.
>
> **Officers**. The officers' category includes current, past and prospective trustees, committee members, and various others involved in the delivery of UKAF winter sport. The personal data we process for officers includes their contact details such as phone numbers, postal addresses and email addresses. It may include notes of discussions regarding day-to-day charity business including records of emails or other message formats. Trustees are likely to have to provide other data to the charity in order to meet the needs of HMRC, the Charity Commissioners or other government agencies.
>
> **Contractors**. The charity contracts services from a number of sources including UK event venues and winter sport providers such as the tourist offices and lift companies of winter sports venues. The personal data we process for contractors is likely to be limited to email addresses and business addresses. It may include notes of discussions regarding day-to-day commercial activity, including records of emails or other message formats.
>
> **Members of UK Armed Forces**. There is a requirement to maintain the contact details of winter sports athletes and other members of the Armed Forces such as senior visitors to events. This is usually restricted to names, ranks, email addresses and phone numbers.

Recipients of Personal Data. UKAFWSA does not anticipate the requirement to share personal data with any other organisation.

Retention Schedule. UKAFWSA will review the database regularly, and not less than annually, with a view to the erasure of personal data which it does not reasonably expect to process in future.

Individual Rights. Individuals have a number of key rights in respect of their data. Although a full explanation of these may be found at https://ico.org.uk/, they include:

- Individuals have the right to be informed about the collection and use of their personal data.

- Individuals have the right to be informed of UKAFWSA's purpose for processing their personal data, the retention period and who it will be shared with. This is called 'privacy information'.
- Individuals have a right to be informed at the time we collect their personal data from them.
- Where we obtain personal data from another source, individuals have a right to be provided with privacy information as soon as is reasonable, and no later than one month.
- The information we provide is to be concise, transparent, intelligible, easily accessible and in clear and plain language.
- Individuals have a right to see the personal data we hold that is about them and to request that mistakes are rectified.
- Individuals have a number of rights to object to the processing of data about them. There is also a specific right to object to direct marketing which we have no grounds to refuse.
- Individuals have a right to lodge a complaint with a 'supervisory authority'. For UK individuals this will be the ICO at https://ico.org.uk/.
- Individuals have a right to block or suppress processing of personal data. In this case, UKAFWSA may still store some data in order to respect the restriction on processing in future.
- Individuals have a right to data portability to allow them to obtain and reuse their personal data for their own purposes across different services.

Where Data is Held. UKAFWSA maintains personal information on the Army Sports Control Board (ASCB) IT system. Personal data is also contained in MOD IT systems and the personal devices or cloud storage folders of our officers.

Automated Decision Making and Profiling. UKAFWSA does not use automated decision making and profiling, including polling.

Opt Out. UKAFWSA offers all the individuals on whom data is held the option to withdraw consent, or 'opt out'. Where such a request is made then UKAFWSA will immediately erase all the data relevant to that individual.

International Transfers. UKAFWSA does not envisage any requirement to transfer personal data for processing beyond the EU, although it is possible that cloud services such as Dropbox may operate beyond the EU[1].

Security Measures. UKAFWSA is content that the security measures applied by the ASCB and MOD on their systems offer adequate and appropriate protection for personal information. For information held by officers on personal devices, UKAFWSA mandates the following security measures:

- **Passwords – Mandatory**. All devices on which personal data is stored must be protected by complex passwords[2], fingerprint or iris recognition technology.

[1] See https://www.dropbox.com/en_GB/security/GDPR
[2] See https://www.cyberaware.gov.uk/passwords

- **Storage – Mandatory**. All information must be stored in a Dropbox folder, or equivalent. This allows users to access the information on their devices when 'off-line' but, importantly, it allows the information to be remotely wiped from a device if it is lost or stolen, whilst not losing the 'cloud' copy of it. It also allows efficient collaborative working and version control, as well as access of the up-to-date versions on other devices such as smartphones.
- **Mobile Storage – Mandatory**. All information held on mobile storage devices such as external hard disks, USB 'thumb' drives or DVDs must be encrypted. The use of such storage is strongly discouraged and should not be necessary if Dropbox is used.
- **Firewall – Mandatory**. Users must activate firewalls on their devices.
- **Malware Protection – Mandatory**. Users must install, enable and keep up-to-date industry-standard malware protection software.
- **Hard Drive Encryption – Strongly Recommended**. Users are recommended to activate or install hard-drive encryption on their devices.
- **Two-Factor Authentication – Strongly Recommended**. Users are strongly recommended to use two-factor authentication to protect their email accounts from access on unauthorised devices.

Officers wishing to hold UKAFWSA personal information on their devices must complete the declaration at Annex B to record their understanding of this policy and the security measures they are to adopt on their devices.

Direct Marketing and Consent. It is not envisaged that UKAFWSA will be engaged in direct marketing activity such as that described in UK Privacy and Electronic Communications Regulations.

Changes to Information. If we plan to use personal data for a new purpose we will update our privacy information and inform individuals before starting any new processing.

Breaches. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

If a personal data breach is detected the outline response plan is to:

- Take any immediate steps (e.g. password changes) to prevent further loss of data.
- Inform the UKAFWSA Board of Trustees immediately.
- Develop an action plan to: allocate responsibilities for action; recover, where possible, the information breach (e.g. find a lost USB stick); learn lessons to prevent further breaches; record the breach; consider communicating the breach to affected individuals based on the risk to them (e.g. if it would make possible identity fraud), and; be prepared to communicate more widely, if appropriate.

- Report the breach to the ICO within 72 hours of its discovery, where it is assessed that there is a risk to individuals' rights and freedoms.

Data Protection Impact Assessment (DPIA). A DPIA will be conducted whenever UKAFWSA adopts new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals. However, it is considered highly unlikely that UKAFWSA will require such technologies.

Privacy Notice for UKAFWSA

UKAFWSA has a requirement to process personal data in order to operate effectively. We will always do so lawfully, fairly and in a transparent manner. Our processes for doing so are reflected in our policy, which is available from our Data Controller, who may be contacted on [insert email address], and is reflected in this privacy notice. Our processes have been developed using the guidance provided by the UK Information Commissioner's Office (ICO).

Scope

This notice refers to our processes for processing personal data in the UK and EU, although information may be stored using cloud services that operate beyond the EU

Our Promise

UKAFWSA will take all reasonable steps to maintain the accuracy of our database of personal data. Where data is found to be inaccurate it will be rectified or erased without delay. We will only collect and store the data for the purposes consistent with the lawful basis described above. We will ensure 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. We do not anticipate a requirement to process the data for archiving purposes in the public interest, scientific, statistical or historical research purposes, although this may be allowable under the law.

Lawful Basis and Legitimate Interests

The lawful basis on which UKAFWSA processes personal data is that we have a legitimate interest to do so. As an Armed Forces' sports charity this means that we are able to maintain effective linkages to representatives of our sponsors and donors ('points of contact'), including prospective sponsors and donors, and better match their needs with those of the charity. We also need to be able to maintain contact with our trustees, officers, volunteers, athletes, contractors, other charities and organisations, and members of the Armed Forces. We must be able to meet the requirements of the Charity Commissioners, HMRC or other government agencies. We do not believe that we can do this in a different way that is less intrusive and we believe that our sponsors, donors and others mentioned above would reasonably expect us to process personal information in this way.

UKAFWSA has a requirement to process the personal data of individuals in four broad categories:

> **Sponsors and Donors**. This category includes current, past and prospective sponsors and donors. These are the representatives of the companies who

support the charity financially or in other ways. The personal data we process for clients includes their contact details such as phone numbers, email addresses, scans of their business cards and details of their support. It may include notes of discussions with them, including records of emails or other message formats.

Officers. The officers' category includes current, past and prospective trustees, committee members, and various others involved in the delivery of UKAF winter sport. The personal data we process for officers includes their contact details such as phone numbers, postal addresses and email addresses. It may include notes of discussions regarding day-to-day charity business including records of emails or other message formats. Trustees are likely to have to provide other data to the charity in order to meet the needs of HMRC, the Charity Commissioners or other government agencies.

Contractors. The charity contracts services from a number of sources including UK event venues and winter sport providers such as the tourist offices and lift companies of winter sports venues. The personal data we process for contractors is likely to be limited to email addresses and business addresses. It may include notes of discussions regarding day-to-day commercial activity, including records of emails or other message formats.

Members of UK Armed Forces. There is a requirement to maintain the contact details of winter sports athletes and other members of the Armed Forces such as senior visitors to events. This is usually restricted to names, ranks, email addresses and phone numbers.

Individual Rights

Individuals have a number of key rights in respect of their data. Although a full explanation of these may be found at https://ico.org.uk/, they include:

- Individuals have the right to be informed about the collection and use of their personal data.
- Individuals have the right to be informed of UKAFWSA' purpose for processing their personal data, the retention period and who it will be shared with. This is called 'privacy information'.
- Individuals have a right to be informed at the time we collect their personal data from them.
- Where we obtain personal data from another sources, individuals have a right to be provided with privacy information as soon as is reasonable, and no later than one month.
- The information we provide is to be concise, transparent, intelligible, easily accessible and in clear and plain language.
- Individuals have a right to see the personal data we hold that is about them and to request that mistakes are rectified.

- Individuals have a number of rights to object to the processing of data about them. There is also a specific right to object to direct marketing which we have no grounds to refuse.
- Individuals have a right to lodge a complaint with a ‘supervisory authority’. For UK individuals this will be the ICO at https://ico.org.uk/.
- Individuals have a right to block or suppress processing of personal data. In this case, UKAFWSA may still store some data in order to respect the restriction on processing in future.
- Individuals have a right to data portability to allow them to obtain and reuse their personal data for their own purposes across different services.

Automated Decision Making and Profiling

UKAFWSA does not use automated decision making and profiling, including polling.

Opt Out

UKAFWSA offers all the individuals on whom data is held the option to withdraw consent, or ‘opt out’. Where such a request is made then UKAFWSA will immediately erase all the data relevant to that individual.

Point of Contact

All questions regarding data protection should be directed to our Data Controller, who may be contacted at [insert email address].

Declaration - Use of Personal Devices

Any officer of the charity wishing to use a personal device (including but not limited to phones, tablets, desktops or laptop computers) to record, store or access personal information about sponsors and donors, officers, contractors or members of the Armed Forces is required to comply with UKAFWSA General Data Protection Regulations (GDPR) policy, including the security measures listed below, as they apply to their various devices. The security measures are:

- **Passwords – Mandatory**. All devices on which personal data is stored must be protected by complex passwords[3], fingerprint or iris recognition technology.
- **Storage – Mandatory**. All UKAFWSA personal data must be stored in a Dropbox folder, or equivalent. This allows users to access the information on their devices when 'off-line' but, importantly, it allows the information to be remotely wiped from a device if it is lost or stolen, whilst not losing the 'cloud' copy of it.
- **Mobile Storage – Mandatory**. All personal data held on mobile storage devices such as external hard disks, USB 'thumb' drives or DVDs must be encrypted. The use of such storage is strongly discouraged and should not be necessary if Dropbox is used.
- **Firewall – Mandatory**. Users must activate firewalls on their devices.
- **Malware Protection – Mandatory**. Users must install, enable and keep up-to-date industry-standard malware protection software.
- **Hard Drive Encryption – Strongly Recommended**. Users are strongly recommended to activate or install hard-drive encryption on their devices.
- **Two-Factor Authentication – Strongly Recommended**. Users are strongly recommended to use two-factor authentication to protect their email accounts and cloud storage accounts from access on unauthorised devices.

_____

Name_____ Rank_____

UKAFWSA Position_____

I agree to comply with UKAFWSA GDPR policy and adopt the security measures described above on any personal device that stores personal information associated with my role in UKAFWSA. I will report the loss of, or unauthorised access to, this information immediately to [insert email address]. I will hand over the information to my successor (or the UKAFWSA Data Controller) and ensure that my authorisation to access it is removed. I will review the information I have access to annually and remove any that is no longer required to fulfil my role.

Signature_____ Date_____

Send completed and signed declarations to [insert email address]

[3] See https://www.cyberaware.gov.uk/passwords