RAF CENTRAL FUND
DATA PROTECTION POLICY

1. Commitment

The RAF Central Fund (the **Fund**) collects and uses information about people with whom it communicates. The Fund is committed to ensuring that any personal information is dealt with properly and securely however it is collected, recorded and used, whether on paper, electronically or recorded on any other material.

The Fund regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals. To this end the Fund fully endorses and adheres to the Principles of Data Protection, as set out in the Data Protection Act 2018, UK GDPR and the EU General Data Protection Regulation (GDPR) (together the Data Protection Legislation).

2. Aim and Status

The aim of this policy is to ensure that the trustees, directors, employees, contractors and volunteers of the Fund are clear about the purpose and principles of Data Protection and to ensure that it has guidelines and procedures in place which are consistently followed.

Any questions or concerns about the operation of this policy should be referred in the first instance to the Head of Marketing and the Head of Operations who may be contacted at mail@rafcf.org.uk.

3. Legislation

The Data Protection Legislation regulates the processing of information relating to living and identifiable individuals (**data subjects**). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems. It is important to read and understand the following terms used in the legislation:

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects, for the purpose of this policy, include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who, or organisations which, determine the purposes for which and the manner in which personal data is processed. They have a responsibility to establish practices and policies in line with the Data Protection Legislation. The Fund is the data controller of all personal data used in our organisation.

Data users include anyone who uses personal data on behalf of the Fund (e.g. employees, workers, volunteers or trustees). Data users have a duty to protect the information they handle

by following our data protection and security policies at all times.

Data processors are the people who, or organisations which, process personal data on behalf of a data controller. This definition does not include our data users but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on thvolune data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Special categories of personal data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sex life, sexual orientation, genetic data, biometric data (used for ID purposes) or criminal convictions, offences or related security measures. Special categories of personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. Principles

Data users must comply with the data protection principles of good practice which underpin the Data Protection Legislation. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this the Fund seeks to follow the six Data Protection Principles outlined in the GDPR, which are summarised below:

- Personal data must be processed lawfully, fairly and in a transparent manner
- Personal data must only be collected for specified, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary
- Personal data must be kept accurate and, where necessary, kept up to date
- Personal data must not be kept for any longer than necessary for the purposes they are processed
- Personal data must be processed in a manner that ensures appropriate security of the personal data, including unauthorised or unlawful processing against accidental loss, destruction or damage, using appropriate technical or organisational measures

Fair and Lawful Processing

The Data Protection Legislation does not prevent the processing of personal data but rather is intended to ensure processing is fair and does not adversely affect the rights of the data subject. In practice this means data subjects must be clear about who the data controller is (in this case the Fund), the purpose for which their data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred. The Fund's public privacy notice contains this information and it is available on our website (www.rafcf.org.uk). The staff privacy notice explains how we collect and use personal data internally.

For personal data to be processed lawfully, certain conditions set out in the Data Protection Legislation have to be met. These may include a requirement that the data subject has

consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When special categories of personal data are being processed, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Data about staff may be processed for legal, personnel, administrative and management purposes and to enable the Fund to meet its legal obligations as an employer, for example to pay staff, monitor their performance and to confer benefits in connection with their employment. Examples of when special categories of personal data of staff are likely to be processed are set out below:

(a) information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;

(b) the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;

(c) in order to comply with legal requirements (e.g. health and safety law) and obligations to third parties.

Collected for specified, explicit and legitimate purposes

Personal data can only be processed for the specific purposes notified to the data subject when their data was first collected or for any other purposes specifically permitted by the Data Protection Legislation. Personal data cannot be used in a manner that is incompatible with those original purposes. This means that personal data cannot be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which personal data is processed, the data subject must be informed of the new purpose before any processing takes place.

Adequate, relevant and limited to what is necessary

Personal data can only be collected to the extent it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place. If personal data becomes irrelevant for the purposes it was collected after a period of time, it should be deleted.

Accurate and, where necessary, kept up to date

Personal data must be kept accurate and up to date. Information which is incorrect or misleading is not accurate. Every reasonable step must be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data must be corrected or destroyed without delay.

Data Retention

Personal data must not be kept longer than necessary for the purposes they are processed. This means that personal data must be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, refer to section 7 below or contact the Fund.

Data Security

We must ensure that appropriate technical or organisational security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss, destruction, or damage to personal data.

Regulations require us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if we have a written agreement in place that meets requirements and the processor agrees to comply with those procedures and policies or has in place adequate measures itself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it;

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed;

(c) **Availability** means that authorised data users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our server instead of individual PCs.

Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Computer hardware such as laptops, desktop computers, memory sticks, mobile devices and CD-ROMs should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users should ensure that computer monitors do not show confidential information to passers-by and that they either lock their screen or log off from their PC when left unattended.

Processing in line with Data Subjects' Rights

Data must always be processed in line with data subjects' rights. Data subjects have a right to:

a) be informed about the collection and use of their personal data by the Fund;

b) access personal data held about them by the Fund;

c) correct inaccurate or incomplete personal data;

d) have personal data erased (also known as ‘the right to be forgotten’)*;

e) to restrict processing of their personal data*;

f) data portability (the right to move, copy or transfer personal data from one IT environment to another in a safe and secure way, without affecting its usability);

g) to object to the processing of their personal data*.

* These rights are not absolute and only apply in certain circumstances.

The GDPR also gives data subjects rights where automated decision-making (including profiling) has a legal or similarly significant effect on them.

Subject Access Requests

The regulations do not specify how to make a valid subject access request and a request can be made verbally or in writing (although it is preferable to obtain confirmation of the request in writing, wherever possible).

Any member of staff, volunteer or contractor who receives a request from a data subject for access to their personal data should notify the Operations Manager and Head of Marketing immediately.

The Fund will usually have 1 month to respond to a subject access request providing the request complies with UK GDPR. In exceptional circumstances (e.g. if the request is complex or the Fund receives a number of requests from an individual) we can extend the time to respond by a further 2 months. The Fund must let the individual know within one month of receiving their request and explain why the extension is necessary.

The time limit should be calculated from the day after the Fund receives the request (whether it is a working day or not) until the corresponding calendar date in the next month. If this is not possible because there is no corresponding calendar date in the following month, the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, the Fund has until the next working day to respond.

If we have any doubts about the identity of the person making the subject access request, we will ask for more information (such as a certified copy of a passport or driving licence and a recent utility bill).
In most cases, the Fund cannot charge a fee to comply with a subject access request. In rare cases where a request is manifestly unfounded or excessive, the regulations permit a reasonable fee to be charged. The Fund will be responsible for making the decision to charge a fee for a subject access request.

5. Scope

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, volunteers, grantees, supporters, suppliers and other third parties. We recognise the need to treat it in an appropriate and lawful manner.

Failure to adhere to the Data Protection Legislation is unlawful and could result enforcement action being taken against the Fund (including a penalty fine of up to €20mn) and/or legal action (including criminal prosecution) being taken against the Fund, trustees or individual data users.

6. Responsibility

During the course of their duties with the Fund, data users may be required to deal with information such as names/addresses/phone numbers/email addresses of grantees/suppliers or other members of staff. All data users must abide by this policy.

The Fund will regard any unlawful breach of any provision of the Data Protection Legislation by any data user as a serious matter which could result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct.

7. Procedures

The following procedures have been developed in order to ensure that the Fund meets its data protection responsibilities.

7.1 Data Records

Purpose
The Fund's privacy notice and data retention schedule explains what personal data we collect from beneficiaries, employees, workers, contractors, volunteers, trustees and committee members and how we use it. The Fund's recruitment privacy notice explains how we collect and use personal information in the recruitment process.

Consent
Consent is only valid if the individual freely takes an active step to indicate their consent – we cannot rely on implied or assumed consent, and we must not pressure someone into giving us consent.

Access
Data including the contact details of staff, volunteers, trustees and committee members will only be accessed internally on a need-to-know basis.

All confidential post must be opened by the addressee only.

Personal data must not normally be passed to anyone outside the Fund without the individual's explicit consent. We may share personal data externally in limited circumstances (for example, where we are under a legal obligation or in emergency situations).

In some circumstances, our suppliers (e.g. IT contractors) may access personal data in the course of providing services to us. We will always ensure that our suppliers provide sufficient

guarantees to meet the requirements of the Data Protection Legislation and that we have a contract with them that meets GDPR requirements.

Requests by beneficiaries, staff, volunteers, trustees and committee members for access to their personal data may be dealt with informally, if the individual agrees. However, any individual has the right to make a formal subject access request to the Fund.

Any staff, volunteers and contractors dealing with enquiries from third parties should be careful about disclosing any personal information held by us. In particular they should:

(a) check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;

(b) suggest they put their request in writing so their identity and entitlement to the information can be verified;

(c) refer to the Operations Manager and Head of Marketing for assistance;

(d) where providing information to a third party, do so in accordance with the six data protection principles.

Accuracy
The Fund will take reasonable steps to keep personal data up to date and accurate. Any request for rectification of incomplete or inaccurate personal data should be addressed without delay and within a maximum of 1 month from the date of the request.

Storage
Personal data is on the Fund's secure IT system.

Every effort is made to ensure that any paper-based data is stored in organised and secure systems.

Use of Photographs
Where appropriate and practicable, the Fund will seek consent from individuals before displaying photographs in which they appear. If this is not practicable (for example, a large group photo), the Fund will rely on its legitimate interests to take and display photographs but we will remove any photograph if an objection is received. This policy also applies to photographs published on the organisation's website.

8. Personal data breaches

Data users must be able to recognise a potential personal data breach. Examples of data breaches include (but are not limited to):

- access by an unauthorised third party (e.g. our computer systems being hacked);
- deliberate or accidental action (or inaction) by the Fund or by a supplier who is acting as a data processor for us;
- sending personal data to an incorrect recipient (for example, sending an email containing a grantee's personal details to the wrong email address);

- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data (for example, systems failing and not having a back-up copy).

Data users must report any potential personal data breach to their line manager or Fund Ambassador. The Fund may be required to report the breach to the Information Commissioner's Office (**ICO**), the Director of RAF Sport, RAF Media, and, in certain circumstances, to notify the individual(s) affected.

Data users should also take any reasonable steps available to reverse or mitigate the effects of a personal data breach (e.g. recalling an email sent to an incorrect recipient or asking someone to return a hard copy of a letter that was not intended for them).

9. Retention of Data

No personal data will be stored for longer than is necessary. For guidelines on retention periods see our Data Retention Schedule. If you have any questions about the retention or deletion of personal data, please speak to the Operations Manager or Head of Marketing.

All documents containing personal data must be disposed of securely in accordance with the Data Protection principles.

10. IT Data Security – HM Government Data

HM Government Data Classifications

HM Government apply three levels of security classification to its information assets, indicating the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. The three levels of classification are currently:

Official - The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

HM Government's definition of Official data includes

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act 2018, UK GDPR, the EU General Data Protection Regulation (GDPR) (together the Data Protection Legislation), or other legislation.

Secret - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

Top Secret – HM Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Official Sensitive - Is a handling caveat for a small subset of information marked Official that require special handling by staff. HM Government guidance[1] confirms that because an Official document or data contains personal information that it should not be marked as Official Sensitive.

Similarly it confirms that aggregation of large amounts of personal data has no bearing on the application of classification markings. Where large data sets of personal information exist in the Official classification, effective procedural, and in some cases technical, controls may be appropriate to reinforce the "need to know" principle and provide enhanced protection. However the data should not be marked Official Sensitive.

The Official Sensitive caveat should only be applied where the "need to know" must be most rigorously enforced, for example, where the loss or compromise of information could have severely damaging consequences for an individual or group of individuals.

HM Government provides the following guidance regarding the sending of ***Official*** personal documents or data via the internet or email:

- Personal information should be protected in transit, i.e. personal information must be encrypted to send across the internet.
- It may be appropriate to send unencrypted personal data over the Internet. Before unencrypted personal information is sent across unsecured networks a risk assessment should be undertaken to assess the consequences of compromise. This assessment should also consider the operational or valid business reasons for this requirement, for example an individual has given permission for their information to be sent via the Internet in order to access or receive a service.
- Aggregated datasets of personal information should never be sent unprotected across unsecured networks.

IT Data Protection Security

To ensure the Fund provides appropriate support to protect HM Government and all personal data requiring protection under the Data Protection Legislation, the following IT systems and safeguards are in place:

Data - all data is fully encrypted in transit.

Server - All Fund information is stored on a secure cloud server in England.

The server consists of two processors, providing separate partitions for the Operating and data systems to segregate the Windows Server license from the main data.

[1] HMG Technology Codes of Practice Guidance (Guidance on handling sensitive information in IT) February 2017

Disaster Recovery System - data is replicated to our bespoke Network Attached Storage ('NAS') device server held by the Funds IT service Providers, CMI.

Data is fully encrypted in flight during transit to the NAS and is not transited outside UK/EEA and is stored in a secure cloud site in England.

UPS - An uninterruptible power supply ensures the server keeps running for sufficient period to protect data loss should there be a power surge or loss of the primary power source.

Network Security - A number of licences are installed on the servers to manage access and security. The Virtual IT Assistant (VITA) utilises an intelligent, integrated software solution to proactively manage the Fund's entire IT infrastructure. If the VITA agent detect an issue or ingress, the Fund is notified of a fault or failure. The Fund utilises VITA add on modules which offer enhanced security monitoring and reporting:

- VITA AV - improved security through centrally monitored anti-virus automated issue logging
- VITA EMM - (Enterprise Mobility Management) provides secure access via centralised security application to Fund mobile laptop users.

Dell SonicWall Firewall - Network security solution providing enterprise grade protection with highly effective intrusion prevention, anti-malware, content/URL filtering and application control. The SonicWall provides secure access to a broad range of mobile devices, including laptops, smartphones and tablets.

Dell SonicPoints - Provide highly effective intrusion prevention as Wireless Access Points for utilisation of Wi-Fi services.

10. Monitoring and Review

The Fund will monitor the effectiveness of this policy regularly considering its suitability, adequacy and effectiveness. As a minimum this policy will be reviewed annually.

The policy does not form part of any contract of employment or other contract for services.