July 2020

WRAC Association Board of Trustees
(incorporating ATS and WRAC Benevolent Fund)

Data Protection Policy - 2020

Policy information	
Organisation	The Women's Royal Army Corps Association (incorporating the ATS and WRAC Benevolent Fund) is registered with the Information Commissioner's Office under registration reference ZA115848.
Terms used in this Policy	WRAC – Women's Royal Army Corps Assoc. – Association ATS – Auxiliary Territorial Service EFC – Executive & Finance Committee ICO – Information Commissioners Office Ben Fund – (ATS & WRAC) Benevolence Fund NI – National Insurance TRBL – The Royal British Legion SSAFA – Soldiers, Sailors, Airmen and Families Association (The Armed Forces Charity) ABF – Army Benevolent Fund DPA – Data Protection Act
Scope of policy	This policy only applies to the WRAC Association (national branch/head-office and its Area Co-ordinators), as registered with the charity commission (206184) (and ICO under registration reference ZA115848). The data held and processed by The Association is for 'Legitimate Purposes' (ie in order to fulfil the charity's obligations, objectives and purposes). All WRAC Branches are independent of the national Association, it's charity commission and ICO registrations. Advice will be issued to Area Co-ordinators and Branch Secretaries, particularly in relation to privacy statements and sharing/not-sharing of members information. The Association uses external agencies for staff payroll and as Administrator for Salesforce (all such external agencies are required to provide a copy of their Data Protection Policy), but does not engage or employ any other data processors.

Policy operational and review dates	This Policy is operational from May 2018 and will be reviewed every three years (with an annual Trustee re-confirmation around May), and amendments made as / when / if required. The next formal review will be May 2021. Minor amendments were made July 2020 to confirm status of Area Co-ordinators, as part of Headquarters Charitable organisation, and therefore their being covered by this Policy.
Policy prepared by	This policy is prepared by the Association Secretary (as Data Protection Officer) and reviewed by the EFC and Trustees.
Date approved by Board/ Management Committee	Approved by Trustees: ……..

Introduction	
Purpose of policy	The data held and processed by The Association is for 'Legitimate Purposes' as recognised by the ICO (ie in order to fulfil the charity's obligations, objectives and purposes). The data held will both comply with the relevant law currently in place as well as follow good practice for an organisation of the Association's size and purposes. The Association holds data such as to legitimately conduct its business – liaising with Members (inc Trustees and Benevolence Fund beneficiaries), staff and contractors – and to comply with Charity Commission and other Regulatory Reporting requirements.
Types of data	The data the Association holds includes: Contact details for: Members Trustees Council Area Co-ordinators Branch Secretaries (or contacts) Benevolence Fund beneficiaries Staff Contractors Contact details include: Name Address Telephone Email (if they have one) Staff NI number employment information (no 'special category' information is kept/stored relating to employees) Nature of contractors' business Benevolence Fund data includes: Beneficiary's contact details Brief note on purpose of grants awarded (In all benevolence cases this information is as supplied to the Assoc. by the associated case-worker organisations, eg TRBL, SSAFA, ABF. The Assoc. does not deal with beneficiaries direct, only through / with approved third-party organisations). This data is used by: Assoc. staff and under specific circumstances, with appropriate permissions, Assoc. Officers (Vice-president, Council, Trustees, Committee Chairs, Area Co-ordinators) Editor of *Lioness* (Members') magazine
Policy statement	The data held and processed by The Association is for 'Legitimate Purposes' as recognised by the ICO (ie in order to fulfil the charity's obligations, objectives and purposes). The data held will both comply with the relevant law currently in place as well as follow good practice for an organisation of the Association's size and purposes.

	The Association holds data such as to legitimately conduct its business – liaising with Members (inc Trustees and Benevolence Fund beneficiaries), staff and contractors – and to comply with Charity Commission and other Regulatory Reporting requirements. The Association will respect individuals' rights and **not** disclose to *any* third party without the express permission of the data subject. The Association will be open and honest to all data subjects about what data it holds on individuals. The Association will provide appropriate training and support to staff in the handling, storage and destruction of data information. The Association will notify the Information Commissioner voluntarily should it be aware of any data protection breaches.
Key risks	The key data risks within the WRAC Association are: ● Individuals considering themselves harmed through data not being updated, thereby being inaccurate or insufficient. However, the Association relies on Members (or associated case-worker organisations, eg TRBL, SSAFA, ABF, in the case of benevolence) to inform it of changes in circumstances, eg contact information. The Association will not change data of its own volition. ● Individuals information being stored or shared inappropriately. (eg external contractor) All data is held on computer, regardless of how it is received.

Responsibilities	
The Trustees Board	The WRAC Association Board of Trustees have overall responsibility for ensuring the Assoc. complies with its legal obligations – delegated to the Executive & Finance Committee and Association Secretary.
Data Protection Officer	The WRAC Association nominated Data Protection Officer is the Association Secretary. Responsibilities will include: Briefing the Board on Data Protection responsibilities Reviewing Data Protection and related policies Advising and training other staff on Data Protection issues Notification to, and liaison with, the ICO Handling subject access requests Consider, and approve if appropriate, unusual or controversial disclosures of personal data
Employees & Volunteers	All staff and appropriate volunteers will be requested to read, understand and accept this Policy and associated procedures. All appropriate staff and volunteers will be given training.

	All Area Co-ordinators and Branch Secretaries will be made aware of this Policy and the procedures that relate to the handling of personal data – and that personal data cannot and will not be shared outside of the Assoc. office without the express permission of the data subject.

Security	
Security measures	All data is held on computer, regardless of how it is received and will be securely stored on computers, which can be shared (by Assoc. staff and Trustees only) using the internally set-up, cloud-based IT-system. Data relating to 'lapsed' Members is stored in a 'lapsed' Member file for two years. After two years information will be 'archived' and only be held for Annual Accounting purposes and for the duration required by law (7 years). Data relating to Benevolence Fund beneficiaries is held on a separate data system (Salesforce) accessible only by the Ben. Fund Secretary and Chairman. All information received and recorded here is as supplied by associated third-party case-worker organisations (eg TRBL, SSAFA, ABF). The data-storage systems used (Capsule and Salesforce) hold information in encrypted form. Passwords are required to access all computers/laptops. Any hard-copy data will be securely stored in locked cabinets and securely destroyed after 6 months, or in the case of employees, 6 months after employment ceases (or as per annual accounts requirements). A record of any amendments received by phone will be written down, dated; and then destroyed after 6 months, at the latest. Association data can only be accessed by the 4 staff and Vice-president. Benevolence Fund data can only be accessed by the Ben. Fund Chairman and Secretary.
Specific risks	The principle risk to subject's data is it being shared inappropriately. For this reason, the Association undertakes **not** to share any information with any third party (except where required for statutory and regulatory reporting requirements), and certain information (such as enquirers' or Members' contact details) will only be shared with Branch Secretaries or Area Chairmen if express permission has been given by the data subject (ie enquirer or Member). NO benevolence fund information will be shared with any branch and/or areas.
Business continuity	Since information is held on cloud-based IT programmes, should there be issues with the physical office becoming unusable, access will still be possible by the 4 staff and Vice-president, in line with physical-office-based procedures.

Data recording and storage	
Accuracy	A record of any amendments received by phone will be written down, dated and destroyed after 6 months, at the latest. Amendments received by email will be appropriately stored on computer, dated and destroyed after 6 months. Amendments received by hard-copy (eg letter) will be appropriately stored, dated and destroyed after 6 months. The Association will endeavour to ensure all data is accurate and up-to-date, but it relies on Members (or associated third-party case-worker organisations (eg TRBL, SSAFA, ABF) in the case of Ben. Fund beneficiaries) to update on individual data (eg change of address). The WRAC Association will not undertake research to verify the accuracy of data information given to it.
Updating	All data is held on computer, regardless of how it is received. Computerised Membership data is checked annually against those who have renewed, or not. Those who have not renewed (subscriptions are due annually) by the following January will be contacted by way or reminder. At this point those not renewing go onto the 'lapsed' list either: until they renew, or they advise to remove their membership, or for two years maximum After two years on the 'lapsed' list the member will be 'archived' or retained as required by annual accounts procedures. Staff information will be retained for the period of employment and six years afterwards, to comply with statutory and regulatory reporting requirements (beyond which it will be securely destroyed). CV's of unsuccessful applicants will be destroyed within six months of application, unless alternative permission has been sought from candidates.
Storage	All data will be securely stored on computers, which can be shared using the internally set-up, cloud-based IT-system. Data relating to 'lapsed' Members is stored in a 'lapsed' Member file for two years. After two years information will only be held for Annual Accounting purposes and for the duration required by law (7 years). Any hard-copy data will be securely stored in locked cabinets and securely destroyed after 6 months, or in the case of employees, 6 years after employment ceases (or as per annual accounts requirements). A record of any amendments received by phone will be written down, dated; and then destroyed after 6 months, at the latest.

	Assoc. data can only be accessed by the 4 staff and Vice-president. Ben. Fund data can only be accessed by the Ben Fund Chairman and Secretary.

Right of Access	
Responsibility	The Association will comply with DPA requirements to allow individuals the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information This will usually be carried out by Assoc. staff as promptly as possible (and definitely within one month).
Procedure for making request	Right of access requests must be in writing, whether by email or letter. All such requests will be provided free of charge – unless there is deemed to be an unnecessary number of requests from one individual, when a small administration charge will be levied. The Association will check a data-subject's identity before handing over information, if they are not known (to ensure there is no breach of data protection)

Transparency	
Commitment	The WRAC Association will ensure that Data Subjects are aware that their data is being processed / held / stored and: Why it is being processed That no disclosures will be made outside the Assoc. and how to exercise their rights in relation to the data
Procedure	The Association will inform data subjects of why and how data is processed by: Employees - the Staff handbook Members – on the Membership Application Form and in the welcome letter, along with occasional reminders in the *Lioness* Trustees and Council – in Induction Pack, along with occasional reminders in Agendas, etc. These will also be supported by information on the Association website.
Privacy Statement	The WRAC Association has a Privacy Statement in place, supporting this Policy. Access to this Statement will be available to all data subjects on the Association website and emails (via a quick-link).

Lawful Basis	
Underlying principles	The WRAC Association holds subject data in order to carry out the Association's 'legitimate business' of running and managing a Membership Organisation and Benevolence fund. The Association's 'legitimate business' includes: Keeping in contact with Members (one of the Assoc's key purposes) through: the Member's magazine (*Lioness*) – distributed twice a year by post, email and available through 'talking newspapers'. Archive versions are also available through the Member's Area of the Association's website. Emails to Members – to pass on news, event-ticket offers and details, gather opinions on certain subjects Telephone – in response to specific enquiries, queries or to pass on specific information Social media – to pass on news and views Liaising with Council and Trustees for: Agendas, Minutes and associated papers To ascertain decisions between meetings (the Association will encourage all email correspondence to be carried out using the Association email address, and / or 'blind copy' emails) This will primarily be by email, and occasionally by post All New Members (those joining after May 2018) will be required to consent to the Association holding and processing their data as part of their joining the WRAC Association. This Consent includes choosing preferred ways of receiving notifications from the Assoc. (email, post, phone). All WRAC Members as at May 2018 will be contacted seeking their specific consent for the Association to contact them using email, post, phone. Photography: The Editor of *Lioness* will consider that all photos sent for consideration for publication in the magazine to have the permission of those in the photograph for its reproduction. Branches will be encouraged to ask people if they do not wish to be included in a photo. Paid staff: Pay and manage personnel In ALL cases, Members, Staff and others will be made aware that the WRAC Association will not share data with any third person organisation or individual. Should such sharing be required (for press and media purposes) each data subject will be approached to give specific permission. No permission given will mean no data will be shared.
Withdrawing consent	The WRAC Association acknowledges that data subjects can withdraw their consent, or the consent for a specified method of contact, at any time (but not retrospectively).

	However, the Association will hold Membership records for 6 months, and staff records information for 6 years, after membership or employed contract has been resigned or lapsed; unless it is required for legal (eg Annual Accounts) purposes.

Employee training & Acceptance of responsibilities	
Induction	The WRAC Association will ensure that all those staff (including appropriate volunteers) who have access to any personal data will have their responsibilities outlined during induction procedures. This will include: Paid staff Vice-president Trustees Council All staff and volunteers will be expected to understand and accept their responsibilities under this Policy, which will be available on the Association computer system and Intranet.
Continuing training	All WRAC Association staff and volunteers who have access to, and process, personal data will be continually reminded of their responsibilities during training, team meetings, staff appraisals, etc.

Policy review	
Responsibility, procedure and timing	This Policy is operational from May 2018 and will be reviewed every three years (with an annual Trustee re-confirmation around May). **The next formal review will be May 2021.** The review will be carried out by the Association Secretary on behalf of the Executive & Finance Committee and Board of Trustees, in liaison with other staff, Vice-president and Trustees.

More information on DPA (data protection) can be found at the ICO website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

(This Policy was designed using a template and guidance from The Emerald Group
(www.emerald-group.co.uk/_userfiles/pages/.../Emerald_Data_Protection_Template.doc
Or search: 'the emerald group GDPR template'