INTRODUCTION TO GOOD GOVERNANCE PROGRAMME

ROYAL AIR FORCES Association

The charity that supports the RAF family

EDINBURGH, LOTHIANS and BORDERS BRANCH

(a charity registered in Scotland No: SC009110)

OSCR Scottish Charity Regulator www.oscr.org.uk Registered Charity SC009110

SCVO

ico. REGISTERED

DATA PROTECTION: GENERAL DATA PROTECTION REGULATION (GDPR) / PRIVACY and ELECTRONIC COMMUNICATIONS (PECR)

BRANCH POLICY DOCUMENT

REVIEW JANUARY 2021

Statement by the Information Commissioner's Office (ICO)

"The UK Government are seeking adequacy decisions from the European Commission. In the absence of adequacy decisions, transfers from the European Economic Area (EEA) to the UK will need to comply with EU GDPR transfer restrictions. We will keep our guidance under review and update it as the situation evolves. There are changes to how to receive personal data from the EU and action you may need to take on data protection. Please continue to monitor the ICO website for updates".

NOTE 1:

On top of the existing legislation, the UK government has issued a statutory instrument titled 'The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019'. In simple terms, this amends the original law and merges it with the requirements of GDPR. The outcome will be a new data protection framework known as the 'UK GDPR'. It is understood that there is virtually no difference between the UK

version of GDPR and the current EU regime. So, for the meantime at least, you should continue to comply with the requirements of the EU GDPR. (ICO 31/12/2020).

NOTE 2:

The outcome of negotiations on the UK's adequacy status is not yet known. Therefore it is well worthwhile ensuring your 'business' is compliant under the current GDPR regime. At the very least, this should help you stay on the right side of the new UK GDPR standard once it's released.(extract from Cyber/Business Resilience January 2021)

NOTE 3:

General comment – It would appear, as previously stated; that there is unlikely to be significant change in UK Domestic UK GDPR for some time, with most of the current debate concerning changes being UK/EU related.(comment: Bob Bertram, Branch Governance/GDPR Lead January 2021)

These Amendments approved by Branch Committee/Trustees on 28th January 2021

George Prentice BEM
Chairman

28/1/2021

Contents

1. CONTACT DETAILS OF ORGANISATION

Edinburgh, Lothians and Borders Branch – RAF Association

contact via:

George Prentice BEM

Branch Chairman/Trustee

Tel: 01890 771230

eMail: chairman@edinburghrafa.org.uk

2. BASIS OF BRANCH DATA PROTECTION POLICY & PROCESSES (GDPR)

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

ASSESSMENT

The Edinburgh, Lothians and Borders Branch of RAFA Committee/Trustees understand the importance of data protection and the impact it can have on individuals and organisations. The Branch Trustees accept their responsibilities under DPA legislation and undertake to comply with the

legislation, guidance/good practice; and in compliance with the RAF Association Personal Data Protection Policy and Standard Operating Procedures.

3. LAWFUL BASIS FOR PROCESSING (AND SHARING)

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

g) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

h) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

i) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

j) Vital interests: the processing is necessary to protect someone's life.

k) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

l) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

ASSESSMENT

As part of this overall review, a 3-part ICO recommended test in relation to 'legitimate interest' **(Legitimate Interest Assessment/LIA)** has been carried out. As a result of this test, the Branch Trustees have re-assessed the relevant lawful basis for processing; and have concluded that the following apply:

'Legitimate Interest' is the most flexible lawful basis for processing, but cannot be assumed to be the most appropriate. It is likely to be most appropriate when individual's personal data is used in ways they would reasonably expect and which have minimal privacy impact, or where there is compelling justification for the processing.

The branch committee/trustees understand that by relying on legitimate they are taking on extra responsibility for considering and protecting people's rights and interests.

The results of the Legitimate Interests Review is published as Annex A. of this document.

4. DATA PROCESSING IMPACT ASSESSMENTS (DPIA)

The GDPR includes an obligation to conduct a DPIA for types of processing to result in a high risk to individuals' interests.

Types of processing that automatically require a DPIA:

- Systematic and extensive profiling with significant effects:
- Large scale use of sensitive data:
- Public monitoring:
- New technologies: processing involving the use of new technologies, or the novel application of existing technologies (including AI).
- Denial of service: Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
- Large-scale profiling: any profiling of individuals on a large scale.
- Biometrics: any processing of biometric data.
- Genetic data: any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.
- Data matching: combining, comparing or matching personal data obtained from multiple sources.
- Invisible processing: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.
- Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
- Targeting of children or other vulnerable individuals: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
- Risk of physical harm: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

<u>ASSESSMENT</u>

A full DPIA Assessment was considered in August 2020 and having reviewed all the types of processing that might result in a high risk to individual's interests; the

Branch Trustees concluded that a full DPIA was not relevant at this time, but this will be re-assessed during any future Review.

The DPIA consideration is published as Annex B. of this document and the full assessment published on the branch website under 'Governance'.

5. PURPOSES and NECESSITY for DATA PROCESSING

The necessity for Data Processing includes the collection, storage and processing of data pertaining to Branch Members and Non-members who have an interest in what we do; and is necessary for enabling contact to keep them up to date with the activities of the branch. In addition, a 'Legal Basis' applies as the branch is registered for Gift-Aid and as such is required to retain and subsequently process claims for gift-aid.

ASSESSMENT

The Trustees have agreed that the Branch should register annually with the Information Commissioner's Office (ICO) as a “Data Controller”. It should be noted that an ICO 'self-assessment' was carried out as part of this review and it confirmed that the Branch Committee/Trustees should continue to be deemed the 'Data Controller' and may act as Data Processor as necessary. The results of this questionnaire also suggested that the operations of the branch could be assessed as 'being exempt' from paying the annual fee for registration, but this can be paid if desired. **This self-assessment is published on the branch website under 'Governance'.**

6. CATEGORIES OF INDIVIDUALS AND CATEGORIES OF PERSONAL DATA

For Branch Members – this data will include Membership Number, Name, Address, Phone Number (if supplied), Email Address (if supplied), Original Membership start date, Expiry date of current membership subscription and type of membership i.e. Ordinary (Full), Associate, Life, Honorary or Serving. It should be noted that branch officers now have access to the RAFA Membership Data Base via the Member's Portal.

For Non-Members – this information can include Email Addresses, Postal Addresses and Telephone Numbers.

7. DATA PROCESSOR OR DATA CONTROLLER ?

Personal data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR applies to ‘controllers’ and ‘processors’.

- a controller determines the purposes and means of processing personal data.
- a processor is responsible for processing personal data on behalf of a controller.

ASSESSMENT

The Branch Committee/Trustees, having re-assessed our use of data and how we process it; have agreed that “for Branch Members and Non-members alike”, the Branch Committee/Trustees are Data Controller and Data Processor as appropriate. In addition, the Trustees assess “Branch Partners” i.e. RAF Air Cadets, 603 RAF Reserve Squadron, Church of the Good Shepherd Murrayfield Edinburgh and local Veterans Breakfast Clubs (and similar) as “organisational entities” and therefore not relating to an “identifiable person”.

For Membership and Non-member purposes the Branch will be a Data Controller and Data Processor as necessary. An individual within the branch should be designated as 'Data Protection Lead', reporting to the Branch Chairman/Branch Committee/Trustees. Other relevant and authorised individuals may be nominated as Branch 'Data Extractors'.

“Data Extractor”- A person who takes data from data sources like the database, which may then be used for further activity. For example, the Membership Secretary and or Branch Secretary running a report to pull off a table of contact details for Branch members; or a person using the database to compile and send out information on events/visits i.e. Branch Social Secretary.

8. DETAILS OF TRANSFERS TO THIRD COUNTRIES

(Not applicable)

9. PRIVACY & ELECTRONIC COMMUNICATIONS REGULATIONS (PECR)

PECR (EC Directive) Regulations 2003, sits alongside the Data Protection Act and GDPR. They give people specific privacy rights in relation to electronic communications. The rules only apply to specific organisations that provide a public electronic communications network or service. The previously issued ADDENDUM to the branch GDPR Policy dated 26 July 2018 still applies i.e. that these rules do not apply to the operations of this branch. **See Annex C. for Branch Assessment.**

10. RETENTION SCHEDULES

These may vary in accordance with the need of “business and other obligations”. However, the basic principle of “no longer than is necessary” will apply. The RAF Association “Personal Data Privacy Standard Operating Procedure (SOP003), Personal Data Retention and Demand” provides detailed guidance on this aspect.

11. DESCRIPTION OF TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The measures taken by the branch to ensure personal data is kept secure include Password protected Personal Computers, limited use of BC email circulations, individual (Trustee) data protection also includes password protected computer facilities, 'Data Traveler USB, and physical security for hard-copy data i.e. address books etc. which will be kept secure. The branch will also comply with the “RAF Association Personal Privacy Policy” currently in force; and this Policy can be read in conjunction with the Association Information Environment Security Policy (ICT Security Policy 1.0), and the relevant Standard Operating Policies (SOP's) – all available on Members Portal (RAFA Website) – under Documents/Policies & Procedures.

NOTE:

Members, volunteers and others with whom Association data has been shared may be personally liable for any breach of DPA/GDPR.

12. RECORDS OF CONSENT

- Individuals can consent to processing; but
- Consent means offering individuals real choice and control
- Consent must be a positive opt-in
- Consent can be withdrawn at any time (by the individual)
- Verbal consent is acceptable (but not encouraged); and must be recorded.
- See Lawful Basis for Processing at 3. above; in addition, a Branch Privacy Notice (Members and Non-members) is published as Annex D.

13. CONTROLLER-PROCESSOR CONTRACTS

Whenever a controller uses a processor it needs to have a written contract in place.

The contract is important so that both parties understand their responsibilities and liabilities.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don’t comply.

ASSESSMENT

Within Edinburgh, Lothians and Borders Branch; a contract exists between the corporate body RAFA and the Branch Committee/Trustees, this contract is renewed annually.

The Branch DPA/GDPR Lead (who may act as Data Processor and Extractor) will “de-facto” may have a documented contract binding himself/herself to another authorised individual within the branch.

No other formal contracts are undertaken by the branch trustees.

14. THE LOCATION OF PERSONAL DATA

(SEE PARAGRAPH 11.)

15. RECORDS OF PERSONAL DATA BREACHES

Any breaches or suspected breaches will be notified to the Information Commissioner within 72 hours; and to Branch Trustees, and RAF Association Data Protection Officer as soon as possible, the results recorded as part of this document.

“A Breach – is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosures of, or access to, personal data”.

“A Serious Breach – results in significant adverse effects of individuals, which include emotional distress, and physical and material damage”.

ADVICE:

“Minimising the information held (e.g. Names and contact details only) restricts the potential damage caused”.

16. INFORMATION REQUIRED FOR PROCESSING SPECIAL CATEGORY DATA OR CRIMINAL CONVICTION AND OFFENCE DATA UNDER THE DATA PROTECTION BILL

a) Generally Not Applicable; however

b) The Branch Honorary Welfare Officers and Assistant Welfare Officers (who may also act as Area Welfare Caseworkers & Befrienders) may record and process special category data (sensitive data) for those of the RAF Family who are experiencing difficulty and requiring the assistance of the Association ; or other relevant charities/agencies. This data is strictly controlled under the RAF Association Data Protection policies by the RAFA Data Controller (the corporate body)

17. BEFORE GDPR

In January 2016 a “Data Pack” was issued to all RAFA Branches & Clubs in relation to the Data Protection Act 1998; and published on the RAFA Website Members Portal. This Policy and related guidelines were circulated to all Branch Committee/Trustees and active volunteers within the branch. In addition; our Branch Membership Secretary registered with the Scotland & NI Area Office as the “Branch Data Processor Lead”. The issue was highlighted at the branch AGM on 24 March 2016 and subsequent branch meetings.

Although the branch were in support of a high level of data protection throughout the Association – there were some concerns that the Policy and Guidelines did not relate to “branch operations” and these concerns were relayed to the RAFA Interim Data Protection Officer accordingly.

18. GDPR 2018

a) In January 2017, due to media exposure, the Branch Trustees became aware of of the General Data Protection Regulation (GDPR) 2018; and as a result made enquiries of the Chief Information Officer at RAF Association Headquarters in Leicester, and also researched the Information Commissioner's (ICO) website. Initially this was to clarify if charities would be subject to these regulations?

   The response received from RAFA HQ was in the affirmative and the branch was advised that guidance would be issued to RAFA Branches in due course.

b) In March 2017 the Chairman of the RAFA Information Environment (IE) Committee issued a draft Personal Data Protection Policy and a number of Standard Operating Procedures (SOP's); this for consultation. The IE Chairman stated “that Personal Data Protection would be strengthened by the implementation of GDPR 2018 and that the Policies and SOP's would be enhanced as they emerged.

c) On 8 March 2017, the RAFA IE Committee issued the updated versions (originals created December 2013) of the Association's Data Protection Policy.

d) At the end of March 2017, the Edinburgh, Lothians and Borders Branch submitted responses to the draft consultation documents. In early April 2017 the branch was advised that some our suggestions had been incorporated into the new documentation, particularly as they affected RAFA Branches themselves.

e) In May 2017, branches were reminded (via Area Newsletters) i.e. “that The Association has a legal obligation to protect personal data in conformance with the Data Protection Act (DPA)1998”; and “that the Association's Data Privacy Policy, together with the associated Standard Operating Procedures, describe the measures necessary for the Association and its members to comply with the DPA”.

In addition; “at branch level this means that any personal data held about branch members must only be used for legitimate Association purposes and that all personal data must be kept under strict control and not inadvertently shared or made available for unauthorised use”.

Branches were also reminded “that the Association is only able to share personal data with branch officials who have agreed to use such data in compliance with the Policy; and have signed the Annual Certificate of Compliance for the protection of personal data”.

It should be noted that the Edinburgh, Lothians and Borders Branch had already complied prior to this reminder being issued from RAF HQ in Leicester – and continued to do so.

f) In February 2018, the Branch Trustees were becoming concerned that no further guidance was being received from RAF HQ. As a result the Branch Interim Chairman and Nominated Data Protection Lead made enquiries of Scotland & NI Area Office and the Chief Information Officer for RAFA in Leicester. This enquiry resulted in advice that DPA/GDPR considerations were still at the Working Party stage; and links to various sources of information on GDPR were given.

At this point, the Trustees agreed that as an independent charity the Branch required to assess the implications of GDPR for itself; and under the guidance and efforts of the Nominated Branch DPA Lead, commenced outlining what the branch required to do to comply with GDPR 2018.

g) On 8 February 2018 the Branch Interim Chairman issued an update on our deliberations to Trustees and Members- these being published in a Branch Quarterly Newsletter and on Branch Facebook page (and thus the Branch Website). This further advised on the forthcoming implementation of GDPR on 25 May 2018; also listing the rights of individuals in relation to this legislation. The paper also advised “that, on the whole, the rights of individuals under GDPR are the same as those under the DPA 1998, but with some significant enhancements”.

In addition, on 25 February, attendees at the Branch Annual General Meeting were advised of GDPR implications and progress to date.

h) Post Branch AGM a small group of Trustees and interested members “brainstormed” where we were with GDPR and formulated an outline Action Plan to take us forward. This Action Plan focused on AWARENESS, INFORMATION HELD, CONSENT, CONTINUED EFFORTS TO RECEIVE BRANCH SPECIFIC GUIDANCE FROM RAFA HQ, WHO WILL BE RESPONSIBLE?; and PRIVACY NOTICES. Thereafter updates on GDPR were provided at every Branch Monthly Meeting.

i) Various email communications between Trustees, Branch Chairman/DPA Lead with RAFA HQ took place; although not ideal- did enhance the branch's understanding of DPA and GDPR.

j) In March 2018 RAFA HQ in Leicester commenced publishing “Branch and Club Communications Papers (General Data Protection Regulation”. These papers covering various aspects of the new regulations.

k) At S&NI Area Conference in Glasgow in April 2018, our HWO, Branch Secretary and Chairman were fortunate to have a conversation with the RAFA Director of Governance; this with a view to clarifying information she shared during her “Governance” presentation at Conference. She provided some interesting and useful clarifications on GDPR that have been incorporated into this document.

l) Due to the dearth of branch specific guidance emanating from RAFA HQ in Leicester; the Branch Trustees were in agreement that the DPA Lead and Chairman should continue with our action plan; and ensure we are complying with the new GDPR, in particular with regard to informing Members and others who for whom we hold data.

m) On 14th May 2018 the Branch DPA Lead & Chairman circulated our agreed Privacy Notice for Members & Non-Members (including Branch Helper/Visitor contacts); these formed Annex. A & B of the original Branch DPA/GDPR Branch Policy Document. At the same time these Privacy Notices were published on the Branch Facebook page and in a prominent position of the Branch Website.

19. CONCLUSION

a) It was expected that the original document would act as a reference for Data Protection compliance in the future and that it would be kept updated and subject to future reviews.

b) In August 2020 the Branch Committee/Trustees agreed that the nominated DPA/GDPR Lead would undertake a full review of the 2018 Branch GDPR Policy Document. This review would include consideration of a Data Protection Impact Assessment, a review of Privacy Notifications for Members & Non Members, Legitimate Interest/Lawful Basis and an assessment of the need to continue registration and the payment of an annual fee to the Information Commissioner's Office (ICO).

c) This review has considered all relevant sources of information: including RAFA, ICO, OSCR guidance and documentation.

d) The draft Review document was submitted to the Branch Committee/Trustees on 24/9/2020 with a subsequent agreement that it be adopted with effect from that date. The new document will be published on the Branch website and available for reference by all.

20. RELEVANT DATA PROTECTION LINKS

Edinburgh, Lothians and Borders Branch RAFA, Website

http://edinburghrafa.org.uk/

Edinburgh, Lothians and Borders Branch RAFA, Facebook page

https://www.facebook.com/RAF-Association-Edinburgh-Lothians-and-Borders-Branch-584393681650950/

RAFA PERSONAL DATA PROTECTION POLICY (on Members Portal)

https://www.rafa.org.uk/

RAFA Privacy Policy

https://www.rafa.org.uk/privacy/

ICO Website

https://ico.org.uk

https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/.

Office of the Scottish Charity Regulator (OSCR)

https://www.oscr.org.uk/managing-a-charity/general-data-protection-regulation-gdpr

21. RECORD OF ONGOING REVUES

VERSION	DATE	ACTION	REASON	PERSON
Draft	May 2020	Draft		Bob Bertram MBE Branch Nominated Data Protection Lead
1.0	September 2020	Publish		Bob Bertram MBE Branch Nominated Data Protection Lead
2.0	January 2021	Amendment	Cover Page Amended	Bob Bertram MBE Branch Nominated Data Protection Lead

ANNEX A.

INTRODUCTION TO GOOD GOVERNANCE PROGRAMME

ROYAL AIR FORCES Association
The charity that supports the RAF family

EDINBURGH, LOTHIANS and BORDERS BRANCH
(a charity registered in Scotland: SC009110)

GDPR 'LEGITIMATE INTEREST' ASSESSMENT (LIA)/CHECKLIST
(as part of the 2020 branch DPA/GDPR Policy Review)

At a glance (extract from ICO guidance)

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:

. identify a legitimate interest;
•show that the processing is necessary to achieve it; and
•balance it against the individual's interests, rights and freedoms.

- The legitimate interests can be your own interests or the interests of third parties.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Identifying 'Legitimate Interest'
The Edinburgh, Lothians and Borders Branch of RAFA is a membership organisation and a registered charity in Scotland (SC009110). It needs to recruit and retain members to ensure the branch is sustainable and also that it requires volunteers for everything it does.

Necessity for Data Processing
The collection, storage and processing of Members and Non-members who have an interest in what we do; is necessary for enabling contact to keep them up to date on the activities of the branch. In addition, branch is registered for 'Gift Aid' and as such is required to retain, subsequently process claims and there is a 'Legal Basis' for data processing.

Individuals Rights and Freedoms
The branch will protect Individuals Rights and Freedoms under the relevant legislation and guidance, particularly in relation to Data Protection/General Data Protection Regulation (GDPR) and Privacy and Electronic Communications Regulations (PECR). Members and Non-members of the branch are deemed to have shared their personal contact details freely, have been informed and reminded of their rights along with advice on how to opt out of receiving electronic and other means of communication. In all our communications with Members and Non-members it is explicit that the branch will only use their personal data as they would reasonably expect.

Checklist (x=completed in the Affirmative)
X We have checked that legitimate interests is the most appropriate basis.
X We understand our responsibility to protect the individual's interests.
X We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
X We have identified the relevant legitimate interests.
X We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
X We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
X We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
X We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
X If we process children's data, we take extra care to make sure we protect their interests.
X We have considered safeguards to reduce the impact where possible.
X We have considered whether we can offer an opt out.
X If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
X We keep our LIA under review, and repeat it if circumstances change.
X We include information about our legitimate interests in our privacy information.

A full Legitimate Interest Assessment (LIA) has been carried out and agreed by the branch Committee/Trustees. This assessment will be published on the Governance page of the branch website. This checklist will form part of the reviewed branch GDPR/PECR policy review document. In addition, Legitimate Interest and Lawful Basis will be included in branch privacy statements.
It should be noted that an Assessment with regard to PECR and its implications for the branch has been carried out separately and will be published on the branch's website and referred to in the Branch Privacy Notice.

Review carried out on behalf of the branch Committee/Trustees (Data Controller).

Bob Bertram MBE
Branch Governance Lead (non trustee)
9 September 2020

ANNEX B.

INTRODUCTION TO GOOD GOVERNANCE PROGRAMME

ROYAL AIR FORCES Association
The charity that supports the RAF family

EDINBURGH, LOTHIANS and BORDERS BRANCH
(a charity registered in Scotland: SC009110)

GENERAL DATA PROTECTION REGULATION (GDPR): DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Introduction
A lesser known requirement of GDPR is that "any time a new project is commenced that is likely to involve 'a high risk' to other people's personal information; a DPIA should be considered by the Data Controller.
Article 35 of GDPR covers DPIA's and states "Where a type of processing in particular using new technologies, and taking into account the purposes of the processing, is likely to result in a high risk to the rights and freedoms of relevant subjects prior to processing, carry out an assessment of the impact of the envisaged processing of personal data".

Background
1. The Edinburgh, Lothians and Borders Branch (committee/trustees) is deemed to be the 'Data Processor' for the purposes of data protection under GDPR; this initially (within the Branch's Data Protection Policy) was solely for 'RAFA Branch Members' and under "legitimate interest".
2. The policy was amended some time ago to nominate the branch as a 'Data Controller' for 'Non-members'.
3. The policy was further amended (in consideration of the impact of Covid-19) to include the branch 'Xmas Card Contact List' and 'Branch Social Contact List'; who may or not be RAFA members.
4. The branch is registered with 'The Information Commissioner's Office (ICO) as a Data Controller for these groups referred to at 2. & 3. above.

Issue(s)
1. Although the descriptions and examples provided in guidance do not appear to apply to our operations as a branch; the guidance also states "it may still be prudent to conduct a DPIA to minimize our liability and ensure best practices for data security and privacy are being followed in our organisation. ***So do it anyway?***
2. This GDPR article refers to "high risk". ***Are our data protection operations 'high risk'?***
3. The branch has already addressed risks in relation to the Xmas Card & Social Contact lists and has decided to include them under "legitimate interest" as per for member – at least during the current Covid-19 pandemic. It is unclear at this time whether this action is strictly legitimate under GDPR; but does provide evidence that under the current pandemic doing so is actively protecting and considering the interests of those who may not be RAFA members – and these decisions have been

made by the committee/trustees in this group's best interest, recorded in the decision minutes and addendums to the branch GDPR Policy formulated, approve and published.

Conclusion(s) (in relation to the above)

1. The necessary actions with regard to DPIA do not appear to apply to the operations of the branch.
2. The operations of the branch under GDPR and the new amendments are not deemed to be 'high risk'.
3. By carrying out this DPIA review, the branch has considered the need for such an assessment and the results of the review will be included in the August 2020 Full Review of the Branch GDPR Policy.

Recommendation(s)

1. That this review is approved by the Branch Committee/Trustees.
2. That this review be included in the Full Branch GDPR August 2020 Review.

Bob Bertram MBE
Branch Life Vice President/Governance Lead

10 August 2020

ANNEX C.

INTRODUCTION TO GOOD GOVERNANCE PROGRAMME

ROYAL AIR FORCES Association
The charity that supports the RAF family

EDINBURGH, LOTHIANS and BORDERS BRANCH
(a charity registered in Scotland: SC009110)

PRIVACY and ELECTRONIC COMMUNICATIONS REGULATIONS (PECR)

BRANCH ASSESSMENT

1. Introduction

PECR are the Privacy and Electronic Communications (EC Directive) Regulations 2003.

The PECR sit alongside the Data Protection Act and the GDPR; and they give people specific privacy rights in relation to electronic communications. There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification; and directory listings.

2. Do PECR apply to me?

Some of the rules only apply to organisations that provide a public electronic communications network or service. **But even if you are not a network or service provider, PECR will apply to you if you:**

- market by phone, email, text or fax;
- use cookies or a similar technology on your website; or
- compile a telephone directory (or a similar public directory).

NOTE:

If emailing Newsletters you need consent to email; this isn't GDPR but PECR. **Newsletters that encourage volunteering, fundraising or promote the work of the organisation are regarded as marketing and email marketing not only has to comply with GDPR but PECR as well. PECR requires 'positive, opt-in consent'** We have been advised that opt-in consent would mainly be an issue for our 'Non-members'; as consent from/for RAFA Members is collected by the corporate body i.e. RAFA

Advice has suggested that key section 44 of PECR 'Direct Marketing' is not

limited to advertising goods or services for sale. It also includes promoting an organisation's aims and ideals. This means that the direct marketing rules in Data Protection and PECR will apply to the promotional, campaigning and fundraising activities of not-for-profit organisations. For example, a charity or political party contacting particular individuals to appeal for funds or votes, or contacting supporters to encourage them to write to their MSP/MP or attend a public meeting or rally, would be covered by the direct marketing. Therefore contacting our Members about their membership or inviting them to an AGM isn't marketing, but other activities would fall within the definition.

(extract from PECR)
"You must not send marketing emails or texts to individuals without specific consent".
Https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/

However; there is an option that has been suggested i.e. that we adopt the 'soft opt-in rule' that would apply to Members of the branch, and also Non-members 'as they provided us with their email details in the first place. It will be incumbent on the branch to ensure both groups are informed 'up front' and this re-iterated in the Branch Privacy Notice. However this can only apply to existing members & non-members i.e. you may be able to email or text your own customers, but it does not apply to to prospective or new contacts. It also does not apply to non-commercial promotions e.g. charity fund-raising or political campaigning.

It would appear that the bottom line and key issue is that "all things data protection are to protect the individual and only use their personal data as they would expect".

Conclusions
It should be noted that the Branch Committee/Trustees considered the implications of PECR in 2018 and on 26 July 2018 an Addendum to the branch GDPR Policy stating "that after due consideration it had been decided that PECR did not apply to the branch". However during the current review of the GDPR Policy, further research and advice from the corporate body RAFA has indicated that PECR does indeed apply to charities and that the implications of 'Marketing' in particular required to be re-considered. In addition; as a practical working option for the required 'consents' in relation to our Members and Non-members, the option of 'Soft Opt-in' has been considered.

As result of this assessment; as Branch Governance Lead I make the following recommendations to the branch committee/trustees.

Recommendation(s)

That the Branch Committee/Trustees agree to the following recommendations and that the results of this assessment will be reflected in the Amended/Updated GDPR Policy document, now to be termed 'Branch Data Protection GDPR/PECR Policy'.

1. That the branch accepts that PECR does apply to the branch and that the implications will be considered in all that we do.
2. That the Branch Privacy Notice to Members & Non-members will make reference to PECR as well as GDPR.
3. That Members and Non-members will be advised and reminded of their rights as individuals in relation to 'soft opt-in' permissions and the right to opt-out at any time.

This PECR Assessment has been carried out in conjunction with a review of the Branch GDPR Policy. This on behalf of the branch Committee/Trustees.

Bob Bertram MBE
Branch Life Vice President/Governance Lead (non trustee)

24 September 2020

ANNEX D.

INTRODUCTION TO GOOD GOVERNANCE PROGRAMME

ROYAL AIR FORCES Association
The charity that supports the RAF family

EDINBURGH, LOTHIANS and BORDERS BRANCH
(a charity registered in Scotland: SC009110)

GENERAL DATA PROTECTION REGULATIONS(GDPR) / PRIVACY and ELECTRONIC COMMUNICATIONS REGULATIONS (PECR): PRIVACY NOTICE TO MEMBERS & NON-MEMBERS OF THE BRANCH

Dear Member/Friend

Whether you are a registered member of the branch, a RAFA member but not a member of this branch or not a member of RAFA but someone who has at some stage expressed an interest in our events and/or the work we do; we are obliged under the above regulations to ensure that you are informed of our branch privacy arrangements and your rights under the above regulations.

Members (of the Edinburgh, Lothians and Borders Branch)
The data (information we hold & process) will, for Members be basic contact information i.e. names, addresses, telephone numbers and email addresses (not sensitive personal data); this data is extracted from the RAF Association Membership Data Base as allowed under these regulations and RAFA policies and procedures. We will use this information to keep in touch with our branch members, to send them branch newsletters, let them know about events and opportunities for fund-raising and volunteering.
It has always been understood that members of RAFA have freely provided this information and that it is accepted 'that the processing of such data is necessary for the legitimate interest of both the member and the branch'.
As a result of the above, there is no requirement for an 'explicit, unambiguous permission statement' from Members. However; members still have the individual right to request that their personal data is not used by the branch for communication/information sharing purposes. If you do not want to receive communications from us, please contact us.
It should be noted however, that although such a request will be honoured by the branch, the member may still receive communications from the corporate body (RAF Association). You can contact The Association to update your preferences at 'privacy@rafa.org.uk'.
NOTE:
The branch welfare team may also collect, store and process personal/sensitive data as part of their role as Branch Honorary Welfare Officers and/or RAFA Welfare Caseworkers/Befrienders. Data Protection arrangements will be controlled and managed by the corporate body The RAF Association.

In terms of 'Privacy of Electronic Communications Regulations (PECR) and relating to Marketing, a 'Soft Opt-in' is allowed i.e. 'existing customers' who have freely given their contact details and did not opt-our of marketing messages are presumed to be content to receive similar information from the branch. However; it is explicit in the PECR rules that a clear opportunity to 'opt-out' must be given, both when details are first collected and in

every such subsequent messages sent.

It should be noted that the branch is registered with the 'Information Commissioner's Office (ICO) as a Data Controller'.

Non-members

The data that we hold for non-members will be restricted to that which you have given us and is generally basic contact information.

Due to the Covid-19 pandemic, the branch committee/trustees were of the view that the branch should use the personal information of non-members to maintain supporting and informative contact with you as non-members, regardless of why you initially provided it to us. As a welfare charity we wanted to make sure that you were OK. The lawful basis for this use of your data was 'legitimate interest'.

Subsequently, as a result of a recent review of the Branch DPA/GDPR Policy it was it was decided to that this arrangement should be formalised and this now forms part of the Branch DPA/GDPR/PECR Policy.

As is the case of Members of the branch, the right not to have your personal data used in this way also applies. If you would like us to stop contacting you, please let us know.

General Privacy Arrangements

- The branch is registered with the Information Commissioner's Office (ICO) as a 'Data Controller'.
- All personal data is held and processed securely as required under the GDPR regulations and RAF Association Policies and Procedures.
- We do not share your personal data with any other person or organisation; except to authorised persons within the RAF Association.
- Such personal data will only be used for your benefit i.e. legitimate interest & lawful basis.
- As previously stated; you have the right to request that your data is not used for these purposes. If this is the case; please contact the branch. However this removal will only be actioned by the Edinburgh, Lothians and Borders Branch. Therefore you may still receive contact/information from the RAF Association itself i.e. the corporate body.

Your Rights under GDPR

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object; and
- the right not to be subject to automated decision-making including profiling

You also have the Right of Access

- Individuals have the right to access their personal data.
- This is commonly referred to as 'subject access'.
- Individuals can make a subject access request verbally or in writing.
- The branch will have one month to respond to a request.
- A fee will not be charged to deal with a request in most circumstances.

In conclusion; and on behalf of the branch Committee/Trustees and myself as Branch Chairman – we take the opportunity to thank you for your continued membership, interest and support.

If you have any questions, please contact me as below; or see:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
or:
www.edinburghrafa.org.uk (under Governance)

George Prentice BEM
email: chairman@edinburghrafa.org.uk

24th September 2020

SCVO