F4H
c/o RHQ RTR
Stanley Barracks,
Bovington, BH20 6JB

www.f4h.org.uk

1 Oct 2018

F4H General Data Protection Regulation (GDPR) – Policy and Management Guidelines

References:

A. European General Data Protection Regulation (GDPR), 25 May 2018.
B. Information Commissioner's Office (ICO) GDPR: https://ico.org.uk/for-organisations/charity/
C. ICO Guide to GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
D. Reporting a Breach: https://ico.org.uk/for-organisations/report-a-breach/

Document Management Record

Originated: May 18

Next Full Document Review Date: Sep 19 (or as/if update required if earlier)

Document Status					
Issue	Date	Notes	Originator	Authorised by	Comments / Version
1	~~8 May 2018~~	~~Initial draft~~	~~CEO~~	~~CEO~~	~~Initial draft for comment~~
2	~~24 May 2018~~	~~Working Draft~~	~~CEO~~	~~CEO~~	~~Working Draft~~
3	Sep 2018	Final	CEO	CEO	V2
4					
5					
6					
7					
8					
9					

Contents

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Introduction

1. This Policy sets out the obligations of F4H, a charity and company registered in the United Kingdom under the name Remount t/a Future for Heroes Ltd (known as F4H), whose registered office is:

C/O The Accountant
RHQ RTR
Stanley Barracks
Bovington
Dorset
BH20 6JB[1].

2. The Policy regards the data protection and the rights of delegates and F4H charity volunteers ('data subjects') in respect of their personal data under the European General Data Protection Regulation (GDPR) 2018, Reference A.

3. The GDPR defines 'personal data' as any information relating to an identified or identifiable natural person (a 'data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

4. This Policy sets the charity's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the charity, its volunteers or other parties working on behalf of the charity.

5. The charity is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Data Protection Principles

6. This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

a. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

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 it is processed.

d. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is 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 is 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 the data subject.

[1] Registered charity: 1126396; Registered Company in England and Wales: 6724674 limited by guarantee.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

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.

7. Furthermore:

a. F4H will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased/destroyed once the need to hold it has passed.

b. Third parties with whom the charity deals (eg, The Brathay Trust and benevolent fund employees) are subject to their own stringent data protection policies and procedures.

c. Potential delegates and delegates will be informed for what reason the data is collected and with whom it might be shared and for what reason (eg, The Brathay Trust / recognised mainstream service (benevolent) charities).

d. No passing of delegates' personal data to any third party will occur unless specific permission has been given (and recorded, see below).

e. Guiding principles for the charity include:

Overriding Data Principles – for consideration regarding our delegates

- PERSONAL INFORMATION IS ONLY USED WITH DELEGATE'S KNOWLEDGE
- ONLY INFORMATION THAT WE ACTUALLY NEED IS COLLECTED
- PERSONAL INFORMATION IS ONLY SEEN BY THOSE WHO NEED IT TO DO THEIR JOBS
- PERSONAL INFORMATION WILL NOT BE PASSED TO ANY OTHER ORGANISATION WITHOUT AGREEMENT UNLESS REQUIRED TO DO SO BY THE LAW
- PERSONAL INFORMATION IS RETAINED ONLY FOR AS LONG AS IT IS REQUIRED
- WE WILL, WHERE NECESSARY, KEEP INFORMATION UP TO DATE
- INFORMATION WILL BE PROTECTED FROM UNAUTHORISED OR ACCIDENTAL DISCLOSURE
- WE WILL PROVIDE DELEGATES WITH A COPY OF THEIR PERSONAL DATA WE HOLD ON REQUEST
- INACCURATE OR MISLEADING DATA WILL BE CORRECTED AS SOON AS POSSIBLE
- THESE PRINCIPLES APPLY WHETHER WE HOLD INFORMATION ON PAPER OR IN ELECTRONIC FORM.

Accountability and Record-Keeping. Data Protection Officer (DPO).

8. No specific DPO is required by the charity. However, the CEO is responsible for the oversight of all data protection concerns and processes; in effect the CEO acts as the Data Controller.

9. The CEO is responsible for overseeing the implementation of this Policy and for monitoring its compliance with the GDPR and other applicable data protection legislation.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

10. The charity shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information (see separate Privacy Notice, also available on our website www.f4h.org.uk):

a. The name and details of the charity, its CEO, and any applicable third-party data processors.

b. The purposes for which the charity collects, holds, and processes personal data.

c. Details of the categories of personal data collected, held, and processed by the charity, and the categories of data subject to which that personal data relates.

d. Details of how long personal data will be retained by the charity; and

e. Detailed descriptions of all technical and organisational measures taken by the charity to ensure the security of personal data.

Data Controller / Processor.

11. Any person that processes data on behalf of the charity/CEO. An MOU is at Annex A; in the spirit of the GDPR 2018, all F4H charity workers and volunteers considered as Data Processors and are to adhere to both the letter and spirit of the MOU.

a. Data Controller. A person who (either alone or jointly or in common with other persons) determines the purpose for which and manner in which ay personal data are, or are to be, processed.

b. Data Processor. Any person[2] (other than an employee of the data controller) who processes the data on behalf of the data controller.

The Rights of Data Subjects

12. The GDPR sets out the following rights applicable to data subjects, details are set out throughout this document:

a. The right to be informed.

b. The right of access.

c. The right to rectification.

d. The right to erasure (also known as the 'right to be forgotten').

e. The right to restrict processing.

f. The right to data portability.

g. The right to object.

h. Rights with respect to automated decision-making and profiling.

Lawful, Fair, and Transparent Data Processing

13. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

a. The data subject has given consent to the processing of their personal data for one or more specific purposes.

Consent can be orally, but a record of the time, date and how (telephone call, face-to-face, text) must be made at the time of the conversation including what was said/agreed. Outreach / Administration must ensure this happens and that the record is accurate.

[2] Volunteer/supporters are not employed by the charity.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

b. The processing is necessary for the performance of a 'contract' to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them.

c. The processing is necessary for compliance with a legal obligation to which the data controller is subject.

d. The processing is necessary to protect the vital interests of the data subject or of another natural person.

e. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

f. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, (in particular where the data subject is a child).

g. If the personal data in question is 'special category data' (also known as 'sensitive personal data', for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

(1) The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so).

(2) The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject).

(3) The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

(4) The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects.

(5) The processing relates to personal data which is clearly made public by the data subject.

(6) The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.

(7) The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

(8) The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with

a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR.

(9) The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

(10) The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Specified, Explicit, and Legitimate Purposes

14. The charity collects and processes personal data. This includes:

a. Personal data collected directly from data subjects.

b. Personal data obtained from third parties if, say, a delegate has been referred to F4H from another organisation. This data is usually limited but will be with the delegate's knowledge from negotiations previously made by the third party with the delegate.

c. The charity only collects, processes, and holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by GDPR).

d. Data subjects are kept informed at all times of the purpose or purposes for which the charity uses their personal data[3].

Adequate, Relevant, and Limited Data Processing

15. The charity will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

Accuracy of Data and Keeping Data Up-to-Date

16. The charity shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date wherever possible. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

17. The accuracy of personal data shall be checked when it is collected. If required and on subsequent checks, for any personal data found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

18. The charity shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed[4].

19. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

Secure Processing

20. The charity shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

[3] This may include such detail included in Course Reports, regarding individual delegates.

[4] This routinely is 5 years to enable us to respond to any questions or complaints, show that we treated the data subject fairly, to maintain records. See separate Privacy Notice. This period can be extended (rarely utilised).

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Further details of the technical and organisational measures which shall be taken are provided elsewhere in this Policy.

Data Protection Impact Assessments

21. A Data Protection Impact Assessment is at Annex B and addresses the following:

    a. The type(s) of personal data that will be collected, held, and processed.

    b. The purpose(s) for which personal data is to be used.

    c. The charity's objectives.

    d. How personal data is to be used.

    e. The parties (internal and/or external) who are to be consulted.

    f. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

    g. Risks posed to data subjects.

    h. Risks posed both within and to the charity; and

    i. Proposed measures to minimise and handle identified risks.

22. Also it is published on our website.

Keeping Data Subjects Informed

23. Every data subject has the right to be informed.

    a. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

    b. Where personal data is obtained from a third party[5], the relevant data subjects then will be informed of its purpose:

        (1) If the personal data is used to communicate with the data subject, when the first communication is made; or

        (2) If the personal data is to be transferred to another party, before that transfer is made; or

        (3) As soon as reasonably possible and in any event not more than one month after the personal data is obtained.

24. The following information can be provided:

    a. Details of the charity.

    b. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing[6,7].

    c. Where applicable, the legitimate interests upon which the charity is justifying its collection and processing of the personal data.

---

[5] As must F4H when referring delegates to third party charities, any third party *should* first have informed the delegate that data would be passed.
[6] Consent and legitimate interest. (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/). 'Consent' initially for course attendance and 'legitimate interest' thereafter (research, etc).
[7] The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data: **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. **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. **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations). **Vital interests**: the processing is necessary to protect someone's life. **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. **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.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

d. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.

e. Where/if the personal data is to be transferred to one or more third parties, details of those parties[8].

f. Details of data retention.

g. Details of the data subject's rights under Reference A[9].

h. Details of the data subject's right to withdraw their consent to the charity's processing of their personal data at any time.

i. Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority').

j. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.

Data Subject Access Request (SAR)

25. Data subjects may make SAR at any time to find out more about the personal data which the charity holds about them, what it is doing with that personal data, and why.

26. Data subjects wishing to make a SAR may do so in writing. SARs should be addressed to the charity through admin@f4H.org.uk. If necessary the SAR will/can be passed to the CEO.

27. Responses to SARs shall normally be made **within one month of receipt**, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

28. All SARs received shall be handled usually in the first instance by Outreach and Administration and, where appropriate, individual relevant charity supporters (mentor/trainers). **In all cases** the CEO should be informed (who will then if necessary provide advice and direction if required) before the SAR is actioned.

29. The charity does not charge a fee for the handling of normal SARs. The charity reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

30. Data subjects have the right to require the charity to rectify any of their personal data that is inaccurate or incomplete.

31. The charity shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the charity of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

32. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

[8] In the case of needy veterans, respective benevolent fund/trust, and, for all delegates, referral to appropriate support organisation, BUT ONLY WITH CONSENT OF delegate (the *status quo*). **Consent must be recorded, see earlier footnote.**

[9] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights. 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 (pass to a third party), The right to object, Rights in relation to automated decision making and profiling.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Erasure of Personal Data

33. Data subjects have the right to request that the charity erases the personal data it holds about them in the following circumstances:

a. It is no longer necessary for the charity to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.

b. The data subject wishes to withdraw their consent to the charity holding and processing their personal data.

c. The data subject objects to the charity holding and processing their personal data (and there is no overriding legitimate interest to allow the charity to continue doing so).

d. The personal data has been processed unlawfully.

e. The personal data needs to be erased in order for the charity to comply with a particular legal obligation.

34. Unless the charity has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

35. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

36. Data subjects may request that the charity ceases processing the personal data it holds about them. If a data subject makes such a request, the charity shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

37. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data Portability

38. Under GDPR data subjects have the right to obtain from F4H their personal information in a format that can be easily re-used. They can also ask us to pass on their personal information in this format to other organisations.

Objections to Personal Data Processing

39. Data subjects have the right to object to the charity processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

40. Where a data subject objects to the charity processing their personal data based on its legitimate interests, the charity shall cease such processing immediately, unless it can be demonstrated that the charity's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

41. **The charity does not process personal data for direct marketing purposes**.

42. Where a data subject objects to the charity processing their personal data for scientific and/or historical research and statistics purposes, the data subject must 'demonstrate grounds relating to his or her particular situation'. The charity is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Automated Decision-Making

43. **The charity does not undertake automated decision-making processes.**

Profiling

44. **The charity does not process personal data for profiling purposes.**

Personal Data Collected, Held, and Processed

45. The following personal data is collected, held, and processed by the charity:

Data Ref.	Type of Data	Purpose of Data
Form A	Personal data – to third party	Evidence of delegate situation and circumstances, for use to secure funding from relevant benevolent fund/trust or appropriate charity. With **consent of delegate.** **Retained by Outreach/Admin only for course attendance purposes then destroyed.** Copy for Accountant only for financial implications and then destroyed.
On-line Application Form[10]	Personal data	To provide details of prospective delegate's situation and purpose for applying for a course. Used by Outreach and Administration.
Course-specific Delegate Attending and Visitor Information sheet	Personal data	Passed to specific course deliverers (trainer, mentor for course requirements) and key charity personnel for reference. To Brathay (central PoC) for technician support, dietary, access and mobility requirements. Central PoC passes specific requirements only to relevant departments: eg, dietary requirements to the chef.
Referral process	Limited Personal data – to third party	Referral to third-party charities/organisations with **consent of delegate.**
Course-specific Course report	Limited personal data	Reporting for charity quality and historical requirements and follow-up procedures (latter with **consent of delegate).**
Mentor Engagement records	Limited personal data	For delegates engaging with mentors, a record to maintain progress (**consent of delegate).**
Follow-up Questionnaires	Personal data	To improve and expand our services, to ensure our course delivery and referral process (where elected) is efficient and suitable for its task. An 'opt in' function.
Charity Volunteers' data	Personal data	PoC, relevant qualifications.

Data Security - Storage

46. Data should be protected at all times, this includes practical approaches such as password protecting IT and locking away laptops when not in use and being meticulous regarding who has access to where data is stored. Overriding principles:

[10] The charity's email is hosted within a secure datacentre on a managed platform which is monitored and regularly updated. All communication with the email server is encrypted, protecting both user credentials and email content in transit. Our website is hosted within a secure datacentre on a managed platform which is regularly updated. All communications with the website are encrypted using an SSL certificate and the website software itself is maintained and regularly updated. (Integrous Ltd, Mar 18).

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

a. All electronic copies of personal data should be stored securely using passwords to secure the information (eg, strong passwords on individual IT to access laptops/work stations).

b. Any, any written or printed information, say for use by course-specific trainers and mentors should be retained for the shortest possible time, suitably protected, and destroyed by either shredding and/or burning as soon as it is no longer required[11].

47. Delegates' course-generated material must be destroyed once no longer required, usually at or by the end of each specific course.

48. Charity personnel shall ensure that the following measures are taken with respect to the storage of personal data:

a. When using IT to store personnel data the principles contained within this document and References should be followed. In addition, all IT systems should be password protected and kept secure when not in use. Use of removable media, which includes removable disks, CDs, USB memory sticks, PDAs and media card formats should be minimised with the same stringent security measures applied.

b. Relevant to Administrator/Outreach: Hard copy versions of collected data must not be kept for longer than one year unless specifically required[12]; advice should be sought if necessary.

c. Personal data may only be transferred to third parties for legitimate reasons outlined here where such parties are known to have stringent data protection policies in force (such as mainstream service charities (eg, respective service benevolent funds) and The Brathay Trust).

Data Security - Transferring Personal Data and Communications

49. The charity shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

a. All emails containing personal data must be encrypted[13].

b. All emails containing personal data must be marked '**CONFIDENTIAL'**.

c. Documents containing personal data must be marked as '**CONFIDENTIAL'.**

d. Personal data contained in the body of an email, whether sent or received, should, if required, be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

e. Rarely, personal data may be sent by facsimile transmission. This is likely to be to an organisation/charity with its own stringent data protection protocols. Where possible, the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

f. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient, **it is not to be posted**.

g. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container, preferably secured.

---

[11] This may not be suitable in the case where individual delegates choose to engage with the mentor. In this case data can be retained as long as the delegate is informed and consent is given – eg Mentor Engagement Records. **Such individual records should thereafter be destroyed IAW the charity's DP Policy or if the data subject no longer wishes the support of a mentor.**

[12] Perhaps in the case where paperwork has been completed but the delegate has not attended a course within one year but it is likely they will.

[13] The charity's email is hosted within a secure datacentre on a managed platform which is monitored and regularly updated. All communication with the email server is encrypted, protecting both user credentials and email content in transit. Our website is hosted within a secure datacentre on a managed platform which is regularly updated. All communications with the website are encrypted using an SSL certificate and the website software itself is maintained and regularly updated. (Integrous Ltd, Mar 18).

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Data Security - Disposal

50. When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

a. Electronic documents – deleted and deleted from Recycle Bin, preferably electronically shredded.

b. Hard-copy shredded/burnt.

c. Emails 'permanently deleted' (and/or 'Deleted Items', 'Bin' immediately deleted thereafter).

Data Security - Use of Personal Data

51. The charity shall ensure that the following measures are taken with respect to the use of personal data:

a. No personal data may be shared informally. If a charity volunteer – other than those specifically requiring access to specific data (eg, course-specific data for respective trainer/mentor) – or other party working on behalf of the charity believe they require access to any additional personal data, such access should be formally requested from the CEO.

b. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.

c. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

d. Where personal data held by the charity is used for further PR opportunities, say with third-party charities, it shall be the responsibility of the CEO to ensure that the appropriate data subject consent is first obtained.

Data Security - IT Security

52. The charity shall ensure that the following measures are taken with respect to IT and information security:

a. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised.

b. Under no circumstances should any passwords be insecurely written down or shared between any charity volunteer, or other parties working on behalf of the charity, irrespective of individuals concerned.

c. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date.

d. No software may be installed on any charity-owned computer or device without the prior approval of the CEO.

e. Regular backing up of personal data should occur. It should be stored only on a password-protected external drive.

F4H Laptop

53. The F4H laptop held at Brathay is not to be used for processing personal data. (Cloud working of personal data can occur once and if the Cloud provider is GDPR-compliant. Details and guidance will follow before initiation occurs).

Organisational Measures

54. The charity shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

a. All individuals volunteering on behalf of the charity shall be made fully aware of both their individual responsibilities and the charity's responsibilities under GDPR and this Policy. They shall be provided with a copy of this Policy.

b. Only individuals volunteering on behalf of the charity or other parties working on behalf of the charity that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the charity.

c. All individuals volunteering on behalf of the charity or other parties working on behalf of the charity shall be required and encouraged to exercise care, caution, and discretion when discussing charity-related matters that relate to personal data.

d. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

e. All personal data held by the charity shall be reviewed periodically.

f. The performance of those individuals volunteering on behalf of the charity or other parties working on behalf of the charity handling personal data shall be regularly evaluated and reviewed.

g. All individuals volunteering on behalf of the charity or other parties working on behalf of the charity handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy.

h. All individuals volunteering on behalf of the charity or other parties working on behalf of the charity handling personal data must ensure that any and all who are involved in the processing of personal data are held to the same conditions as those of the charity arising out of this Policy and the GDPR; and

i. Where other parties working on behalf of the charity handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the charity against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Transferring Personal Data to a Country Outside the EEA

55. The charity does not transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

Data Breach Notification

56. **All personal data breaches must be reported immediately to the CEO**. See Annex C for details of reporting requirements.

57. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (eg, financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the CEO must ensure that the ICO is informed of the breach without delay, and in any event, **within 72 hours after having become aware of it**.[14]

58. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the CEO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

59. Data breach notifications shall include the following information:

a. The categories and approximate number of data subjects concerned.

b. The categories and approximate number of personal data records concerned.

[14] It is essential, therefore, that the CEO is informed of any data breach immediately.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

c. The name and contact details of the charity's CEO (or other contact point where more information can be obtained).

d. The likely consequences of the breach.

e. Details of the measures taken, or proposed to be taken, by the charity to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Annexes:

A. Data Processor – MOU.
B. Data Protection Impact Assessment.
C. Data Breach – Reporting.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Data Controller / Processor MOU

1. In accordance with Article 28 of Reference A, this Annex draws up an MOU between Remount t/a Future for Heroes Ltd (AKA F4H) and the Data Processor [each *individual charity volunteer*[15]].

2. This Agreement is to ensure there is in place proper arrangements relating to personal data passed between F4H and a data processor.

3. The Data Processor agrees to process the data only in accordance with Data Protection Laws, this document and in particular on the following conditions:

   a. The Processor shall only process the data:

      (1) On the written instructions from F4H (this MOU).

      (2) For the use by and within F4H and its role.

      (3) In the UK with no transfer of the data outside of the UK.

   b. The Processor agrees to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

      (1) Consideration of anonymisation and encryption (pseudonymisation is not acceptable).

      (2) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and related services.

      (3) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (backing up data).

      (4) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.

      (5) The Processor is to ensure that anyone acting on their behalf does not process any of the data unless following instructions from F4H unless they are required to do so under English law.

   c. The Processor shall not involve any third party in the processing of the data without the consent of F4H.

   d. Taking into account the nature of the processing, assist F4H by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of F4H's obligation to respond to requests from individuals exercising their rights IAW Reference A.

   e. Assist F4H in ensuring compliance with the obligations regarding security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments, taking into account the nature of processing and the information available to the Processor.

   f. At F4H's discretion, instruction and choice, safely delete or return the Data at any time. (The Processor will in any event securely delete the data at the end of their time with the charity).

      (1) Where the Processor is to delete the data, deletion shall include destruction of all existing copies unless otherwise a legal requirement to retain the data.

[15] Each volunteer/charity worker is to adhere to the letter and spirit of this MOU.

(2) Upon request by F4H the Processor shall provide certification of destruction of all data.

g. Make immediately available to F4H all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by F4H from time to time.

h. Maintain the integrity of the data, ensuring that the data can be separated from any other information created.

i. **Immediately contact F4H/CEO if there is any personal data breach or incident where the data may have been compromised**.

4. F4H may immediately terminate this Agreement on written notice to the Processor. The Processor may not terminate this Agreement without the written consent of F4H.

5. This Agreement may only be varied with the written consent of both parties.

For and on behalf of F4H

Graham Brown CEO

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Data Protection Impact Assessment.

1. See Separate stand-alone document; also available on our website.

The protection of personal data is everyone's business. All staff and volunteers must be vigilant, comply with the policy and report any concerns or occurrences without delay.

Data Breach – Reporting

DATA BREACH INCIDENT REPORTING FORM		
	(a)	(b)
SUMMARY OF INCIDENT		
1.	Date and time of Incident.	
2.	Number of people whose data is affected:	
3.	Department the Incident occurred in:	
4.	Nature of the breach i.e. technical/theft/disclosure error:	
5.	Description of how the error occurred:	
6.	Has the incident been added to the Data Breach Incident Log?:	
REPORTING		
7.	How did you become aware of the breach?:	
8.	Has the Data Protection Officer/Specialist been informed?:	
PERSONAL DATA		
9.	Provide a full description of the personal data involved (without identifying any individuals):	
10.	Have all affected individuals been informed?	
11.	If not, state why:	

DATA BREACH INCIDENT REPORTING FORM		
	(a)	(b)
12.	Is there any evidence to suggest that the personal data involved in this incident has been inappropriately processed or has been further disclosed? If so please provide details:	
DATA RETRIEVAL		
13.	What immediate action was taken?:	
14.	Has the data been retrieved or deleted? If yes please provide the date and time this was done:	
IMPACT		
15.	Describe the risk of harm to the individual as a result of this incident:	
16.	Describe the risk of identity fraud as a result of this incident:	
17.	Have you received a formal complaint from any individual affected by this breach? If so, please provide details:	
MANAGEMENT		
18.	Do you consider the processor involved has breached data governance policies and procedures?:	
19.	Has any disciplinary action been carried out towards the processor involved?:	
20.	Has the processor signed the Controller/Processor MOU of processing?	
21.	Has the processor received adequate and up to date	

DATA BREACH INCIDENT REPORTING FORM		
	(a)	(b)
	training on data protection?:	
22.	Has a Data Protection Impact Assessment been carried out to mitigate any further risk?:	
23.	Has a full investigation been carried out?:	
24.	Has a full report been written on the incident?	
25.	Does the breach need to be reported to the ICO within 72 hours?	