Ellen MacArthur Cancer Trust

Data Protection Policy

1. Introduction

This Policy sets out the obligations of Ellen MacArthur Cancer Trust ("the Trust") regarding data protection and the rights of Young People who sail with the Trust and their Families, Volunteers, Supporters, Suppliers, Contractors (including Skippers), Stakeholders, Donors, Staff and Trustees/Company Secretary) ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation 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.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Trust, its employees, agents, volunteers, contractors, or other parties engaged on behalf of the Trust.

The Trust 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.

PLEASE NOTE that this Policy is likely to be updated from time to time and so you should please access the current version on the Trust's website www.ellenmacarthurcancertrust.org

2. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation 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 they are 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 Regulation in order to safeguard the rights and freedoms of the data subject;

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.

3. Lawful, Fair, and Transparent Data Processing

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

a) the data subject has given consent ("Consent") to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract ("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;

c) processing is necessary for compliance with a legal obligation ("Legal Obligation") to which the controller is subject;

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

e) 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 controller;

f) processing is necessary for the purposes of the legitimate interests ("Legitimate Interest") pursued by the 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.

3.2 Some types of personal data (called "Special Category") are more sensitive, such as that regarding health and sexual orientation. With that data, the processing has to have at least one of the six lawful bases set out at clause 3.1 above which, as regards the Special Category data to be provided to the Trust, is Consent. The data subject must have given explicit consent to the processing of that data.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 The Trust collects and processes the personal data set out in Part 18 of this Policy. This may include personal data received directly from data subjects for

example:

(a) The Trust has both a Legitimate Interest (so to be able to maintain contact) and a Lawful Obligation (by example, Health & Safety and Safeguarding) in the provision by a Young Person (and if, under 18, that of their parent or guardian) of their contact details and needs their Consent as to the processing of that Young Person's health (and any other Special Category) data. On some occasions, it will also be necessary to obtain a Medical Risk Assessment Form from that Young Person's hospital or treatment centre which will also be subject to their Consent;

(b) With a Volunteer, the Trust has both a Legitimate Interest (so to be able to maintain contact) and a Lawful Obligation (by example, Health & Safety and Safeguarding) as to the provision and processing of their contact details and will need their Consent as to the processing of their health data.

(c) With those others who may participate on a Trust trip or event (additional to a Young Person or Volunteer), the Trust has (i) a Legitimate Interest (so to be able to maintain contact) (ii) a Lawful Obligation (by example, Health & Safety and Safeguarding) and (iii) in some instances, a Contract as to the provision and processing of their contact details. The Trust will also need their Consent to the processing of their health data;

(d) The Trust has (i) a Legitimate Interest (so to be able to maintain contact) (ii) a Lawful Obligation (by example, HMRC) and (iii) in some instances a Contract as to the provision and processing of the contact details for the Trust's Donors, Stakeholders, Staff and Trustees/Company Secretary. The Trust will need the Consent of the staff to the processing of their health data as well as that of any other persons that come within this class in the event that they are, in effect, acting as a Volunteer.

4.2 The Trust only processes personal data for the specific purposes set out in Part 18 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which the Trust processes personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, within a reasonable period (being not more than one calendar month) after collection where it is obtained from a third party.

5. Adequate, Relevant and Limited Data Processing

5.1 The Trust will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4 above and which includes the specific purposes set out in Part 18.

5.2 The Trust may pass personal data to third parties (such as outdoor activity centres) to enable them to provide services associated with the activities of the Trust. In such circumstances, the Trust will only disclose the personal data that is necessary for the provision of that service and will have a contract with that provider whereby it is to keep that data secure with it not being allowed to use it for any other purpose, such as marketing.

6. Accuracy of Data and Keeping Data Up To Date

The Trust shall ensure that all personal data collected and processed is kept accurate

and up-to-date. The accuracy of data shall be checked when it is collected and at appropriate intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing

The Trust shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. Secure Processing

The Trust shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 19 and 20 of this Policy.

9. Accountability

9.1 The Trust's Data Protection Lead is Frank Fletcher, frank@emcancertrust.org 01983 297750.

9.2 The Trust shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the Trust, its Data Protection Lead, and any applicable third-party data controllers;

b) The purposes for which the Trust processes personal data;

c) Details of the categories of personal data collected, held, and processed by the Trust; and the categories of data subject to which that personal data relates;

d) Details (and categories) of any third parties that will receive personal data from the Trust;

e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

f) Details of how long personal data will be retained by the Trust; and

g) Detailed descriptions of all technical and organisational measures taken by the Trust to ensure the security of personal data.

10. Privacy Impact Assessments

The Trust shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Trust's Data Protection Lead and shall address the following areas of importance:

10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

10.2 Details of the legitimate interests being pursued by the Trust;

10.3 An assessment of the necessity and proportionality of the data processing with

respect to the purpose(s) for which it is being processed;

10.4 An assessment of the risks posed to individual data subjects; and

10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

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.

12. Keeping Data Subjects Informed

12.1 The Trust shall ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the Trust including, but not limited to, the identity of Frank Fletcher, its Data Protection Lead;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the Trust is justifying its collection and processing of the personal data;

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

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 21 of this Policy for further details concerning such third country data transfers);

g) Details of the length of time the personal data will be held by the Trust (or, where there is no predetermined period, details of how that length of time will be determined);

h) Details of the data subject's rights under the Regulation;

i) Details of the data subject's right to withdraw their consent to the Trust's

processing of the personal data relating to their health at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

k) 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;

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;

12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication; or

b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c) In any event, not more than one month after the time at which the Trust obtains the personal data.

13. Data Subject Access

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Trust holds about them. The Trust is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.2 All subject access requests received must be forwarded to Frank Fletcher, the Trust's Data Protection Lead frank@emcancertrust.org

13.3 The Trust does not charge a fee for the handling of normal SARs. The Trust 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.

14. Rectification of Personal Data

14.1 If a data subject informs the Trust that personal data held by the Trust is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data

subject shall be informed of the need for the extension).

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

15. Erasure of Personal Data

15.1 Data subjects may request that the Trust erases the personal data it holds about them in the following circumstances:

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

b) The data subject wishes to withdraw their consent to the Trust holding and processing the personal data relating to their health;

c) The data subject objects to the Trust holding and processing their personal data that does not relate to their health (and there is no overriding legitimate interest or legal obligation to allow the Trust to continue doing so) (see Part 17 of this Policy for further details concerning data subjects' rights to object);

d) The personal data has been processed unlawfully;

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

15.2 Unless the Trust 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 (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject 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).

16. Restriction of Personal Data Processing

16.1 Subject to clause 17.2 below, data subjects may request that the Trust ceases processing the personal data it holds about them. If a data subject makes such a request, the Trust shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2 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).

17. Objections to Personal Data Processing

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

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

17.3 Where a data subject objects to the Trust processing their personal data for direct marketing purposes, the Trust shall cease such processing forthwith.

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

18. Personal Data

The following personal data may be collected, held, and processed by the Trust:

a) Medical information of those joining the Trust's trips (or otherwise acting as a Volunteer or being a member of the Trust's staff) as part of its safety management process;

b) Personal information of Donors to process donations and retail payments;

c) Personal information on Staff to process the Trust's payroll;

d) Personal information on Staff, Contractors and Volunteers to undertake Disclosure and Barring Service checks (known as the Protecting Vulnerable Groups Scheme in Scotland). The Trust has a separate Ex-Offenders Policy which is available on request;

e) Personal contact information of Volunteers, Contractors, Trustees/Company Secretary and Staff to aid the smooth running of the Trust;

f) And other information in the pursuit of the Trust's charitable aims.

19. Data Protection Measures

The Trust shall ensure that all its employees, agents, contractors, or other parties engaged on its behalf comply with the following when engaged with personal data:

a) Where 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, in the absence of solid state drives, be securely deleted and disposed of. Hard disk drives and all hardcopies should be destroyed or shredded, and electronic copies should be deleted securely;

b) Personal data may be transmitted over secure networks only (such as by way of an email sent from and to the Trust's email address); transmission over unsecured networks is not permitted in any circumstances;

c) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

d) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail;

e) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party engaged on behalf of the Trust requires access to any personal data that they do not already have access to, such access should be formally requested from Frank Fletcher CEO: frank@emcancertrust.org;

f) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

g) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are engaged on behalf of the Trust or not, without the authorisation of Frank Fletcher CEO: frank@emcancertrust.org;

h) 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;

i) 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;

j) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Trust or otherwise without the formal written approval of Frank Fletcher CEO frank@emcancertrust.org and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

k) No personal data should be transferred to any device personally belonging to an employee. Personal data may only be transferred to devices belonging to agents, contractors, or other parties engaged on behalf of the Trust where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Trust that all suitable technical and organisational measures have been taken);

l) All personal data stored electronically should be backed up on the Trust servers with backups stored onsite, with the exception of Salesforce and Office 365 where backups will reside on the host's servers;

m) All electronic copies of personal data should be stored securely using passwords;

n) All passwords used to protect personal data should be generated by, and stored in, the Trust's password management solution. These random computer-generated passwords should be a minimum of 16 characters in length and contain a combination of uppercase and lowercase letters, numbers and symbols. The user generated password for each users 'vault' in the Trust password manager should be a minimum of 24 characters and should be changed every 90 days unless two-factor authentication is in place.";

o) Under no circumstances should any passwords be written down. The sharing of passwords with agents, contractors or other parties engaged on behalf of the Trust is prohibited. Where passwords have to be shared within the Trust this should be accomplished through the password sharing functionality in the Trust's password management solution where it can be audited. If a password is forgotten, it must be reset using the applicable method. The Trust's IT personnel do not have direct access to passwords.;

p) Where personal data held by the Trust is used for marketing purposes, it shall be the responsibility of Frank Fletcher CEO and Tanya Brookfield, Head of Fundraising and Communications to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Fundraising Preference Service, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually. Any requests received by the Fundraising preference service must be dealt with within 30 days.

NB: Two-factor authentication will be used further to secure access to accounts where this facility is an available option.

20. **Organisational Measures**

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

a) All employees, volunteers, agents, contractors, or other parties engaged on behalf of the Trust shall be made fully aware of both their individual responsibilities and the Trust's responsibilities under the Regulation and under this Policy by way of links being provided to both;

b) Only employees, volunteers, agents, contractors, or other parties engaged on behalf of the Trust 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 Trust;

c) All employees, volunteers, agents, contractors, or other parties engaged on behalf of the Trust handling personal data will be appropriately trained to do so;

d) All employees, volunteers, agents, contractors, or other parties engaged on behalf of the Trust handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, volunteers, agents, contractors, or other parties engaged on behalf of the Trust handling personal data shall be regularly evaluated and reviewed;

g) All employees, volunteers, agents, contractors, or other parties engaged on behalf of the Trust handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, volunteers, contractors, or other parties engaged on behalf of the Trust handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Trust arising out of this Policy and the Regulation;

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

21. Transferring Personal Data to a Country Outside the EEA

21.1 The Trust may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

21.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) The transfer is made with the informed consent of the relevant data subject(s);

d) The transfer is necessary for the performance of a contract between the data subject and the Trust (or for pre-contractual steps taken at the request of the data subject);

e) The transfer is necessary for important public interest reasons;

f) The transfer is necessary for the conduct of legal claims;

g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

22. Data Breach Notification

22.1 All personal data breaches must be reported immediately to the Trust's Data Protection Lead.

22.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Lead must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

22.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 22.2) to the rights and freedoms of data subjects, the Data Protection Lead must ensure that all affected data

subjects are informed of the breach directly and without undue delay.

22.4 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;

c) The name and contact details of the Trust's Data Protection Lead (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 Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

23. Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by the Trustees of Ellen MacArthur Cancer Trust.