THE DATA PROTECTION POLICY

of the

FINDHORN FOUNDATION ("FF")

1. Policy Statement

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

1.2 Any breach of this policy will be taken seriously and may result in disciplinary action.

2. About This Policy

2.1 The types of information that we may be required to handle include details of current, past and prospective employees, programme participants, prospective guests and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulations ("GDPR") and other regulations. GDPR imposes restrictions on how we may use that information.

2.2 This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal data and information.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 The Compliance Officer is responsible for ensuring compliance with the GDPR and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the Compliance Officer.

2.5 If you consider that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with your line manager or the Compliance Officer.

3. Definitions of Data Protection Terms

3.1 **Automated Decision Making** ("ADM") is when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. GDPR prohibits ADM (unless certain conditions are met) but not automated processing.

3.2 **Automated processing** is any form of automated processing Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

3.3 **Consent** is agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of Personal Data relating to them.

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

3.5 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with GDPR. FF is the data controller of all personal data used in our business.

3.6 **Data Privacy Impact Assessment** ("DPIA") is tools and assessments used to identify and reduce risks of an earlier processing activity. DPIA can be carried out as part of the Privacy by Design and should be conducted for all major system or business programmes involving the processing of Personal Data.

3.7 **Data processors** include any person who processes personal data on behalf of a data

controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.8 **Data Protection Officer** ("DPO") is the person required to be appointed under specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a DPO or other voluntary appointment of a DPO or refers to the data privacy team who is responsible for data protection compliance. There is no DPO appointed at FF.

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

3.10 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.11 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data and excludes anonymous data or data which had the identity of an individual permanently removed.

3.12 **Personal Data Breach** is any act or omission which compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that FF or its third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

3.13 Privacy by Design is implementing appropriate technical organizational measures in an effective manner to ensure compliance with GDPR.

3.14 Privacy Notices or Privacy Policies are separate notices setting out information that may be provided to Data Subjects when FF collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy or the guest privacy notice for

attendance and participation in programmes) or they may be stand-alone one time privacy statements covering Processing relating to a specific purpose.

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

3.16 Pseudonymisation is replacing information which directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is supposed to be kept separately or secure.

3.17 Sensitive Personal Data includes information and data about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual orientation, biometric or genetic data, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the unambiguous consent of the person concerned unless one of the other lawful exceptions applies.

4. Personal Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully and in a transparent manner;

(b) Collected and processed for specific legitimate purposes and in an appropriate way;

(c) Adequate, relevant and not excessive for the purpose;

(d) Accurate;

(e) Not kept longer than necessary for the specific purpose or for regulatory purposes;

(f) Processed in line with data subjects' rights and accessible to the data subject;

(g) Secure and safe using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage;

(h) Not transferred to people or organisations situated in countries without adequate protection and safeguards.

5. Fair And Lawful Processing

5.1 GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case The Findhorn Foundation), who the data controller's representative is (in this case the Compliance Officer), the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has unambiguously consented to the processing, or that the processing is necessary for the performance of a contract or other legitimate purpose by the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In some cases the data subject's unambiguous consent to the processing of such data will be required.

5.3 Data about staff may be processed for legal, personnel, administrative and management purposes and to enable the data controller to meet its legal obligations as an employer, for example to pay staff, monitor their performance and to confer benefits in connection with their employment and for health and safety reasons. Some examples of when sensitive personal data of staff is likely to be processed are set out below:

(a) Information about an employee’s physical or mental health or condition in order to

monitor sick leave and take decisions as to the employee's fitness for work;

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

(c) In order to comply with legal requirements and obligations to the data subject and/or third parties.

5.4 Data about programme participants and other third parties may be processed in accordance with the Findhorn Foundation's privacy policy.

6. Processing For Limited Purposes

Personal data will only be processed for the specific purposes notified to the data subject when the data was collected or for any other purposes specifically permitted by GDPR. This means that personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

7. Adequate, Relevant And Non-excessive Processing

Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose will not be collected in the first place. In particular staff should consider:

(a) Do I really need this information about an individual? Do I know what I'm going to use it for? When do I delete/destroy personal data and information?

(b) Am I sure the personal data or information is accurate and up to date?

(c) Do the people whose information and data I hold know that I have got it and are they likely to understand what it will be used for? Would any of them be surprised at what I'm doing with their personal data and information?

(d) If I'm asked to pass on personal data or information am I sure it's okay to do so? If in

doubt, I will ask when personal data or information can be passed on.

(e) Am I satisfied that personal data or information is being held securely, whether it's on paper or computer?

(f) Is access to personal data or information limited only to those with a strict need to know? Have I thought about who's actually going to be able to see the personal data or information?

8. Accurate Data

Personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be rectified or destroyed.

9. Data Retention

Personal data will not be kept longer than is necessary for the specific purpose or for the purpose of compliance with legal regulatory, accounting or other legitimate reporting obligations. This means that data will be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Compliance Officer.

10. Processing In Line With Data Subjects' Rights

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

(a) Request access to any data held about them by a data controller;

(b) Prevent the processing of their data for direct-marketing purposes;

(c) Ask to have inaccurate data amended, rectified or erased;

(d) Prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else;

(e) Object to any decision that significantly affects them being taken solely by a computer or other automated process;

(f) Withdraw consent to processing at any time.

11. Data Security

11.1 FF will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2 GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures and safeguards.

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

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

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

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

11.4 All employees with access to Personal Data must comply with all applicable aspects of the FF data protection policies and must not attempt to circumvent the administrative, physical and technical safeguards implemented by FF and maintained in accordance with the GDPR and relevant standards to protect Personal Data.

11.5 Security procedures include:

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

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

(c) Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

(d) Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

11.6 A Personal Data Breach:

(a) GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

(b) FF has put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject of any applicable regulator where FF is legally required to do so.

(c) If any employee knows or suspects that a Personal Data Breach has occurred they should immediately contact the Compliance Officer or the person or team designated as the key point of contact for Personal Data Breaches.

12. Subject Access Requests

A formal request from a data subject for information that we hold about them must be made in writing. Any member of staff who receives a written request should forward it to the Compliance Officer immediately.

13. Providing Information To Third Parties

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal data or information held by us. In particular they should:

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

(b) Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified.

(c) Refer to the Compliance Officer for assistance in difficult situations.

14. Transfer Limitation

(a) Where providing information to a third party, do so in accordance with the eight data protection principles.

(b) GDPR restricts data transfers to countries outside the EEA to make sure the level of data protection for the two individuals by GDPR is not undermined. Personal Data may only be transferred outside the EEA if one of the following conditions applies:

(i) The European Commission has issued a decision confirming that the country to which Personal Data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(ii) Appropriate safeguards are in place such as binding corporate rules, standard contractual clauses proved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Compliance Officer;

(iii) The Data Subject has provided an unambiguous consent to the proposed transfer after being informed of any potential risks; or

(iv) The transfer is necessary for one of the other reasons set out in the GDPR

including the performance of a contract between FF and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect a vital interest of the Data Subject where the Data Subject is physically or legally incapable of giving consent and, in some limited cases, for FF's legitimate interests.

15. Monitoring And Review Of The Policy

This policy is reviewed annually by the Compliance Officer to ensure it is achieving its stated objectives. Recommendations for any amendments are reported to the Compliance Officer.

GDPR requires FF to keep full and accurate records of all Data Processing activities. FF is required to ensure that all personnel have undergone adequate training to enable them to comply with data privacy laws. FF must also regularly test its systems and processes to assess compliance. All employees must undertake mandatory data privacy related training when required. Systems and processes will be regularly reviewed to ensure they comply with GDPR and the FF privacy policies and privacy notice standards.

16. Direct Marketing

FF is subject to certain rules and privacy laws when advertising and marketing services and programmes to members of the public and prospective guests and programme users. A data subject's prior unambiguous consent is required for electronic direct marketing (for example by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows FF to send marketing letters, texts or emails if that Personal Data has been obtained in the course of a previous communication or sale of services to that person and FF is marketing similar products or services and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be specifically offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honored and acted upon. If a customer or member of a marketing mailing list opts out at any time, their details should be suppressed as

soon as possible. The suppression involves making sure that marketing preferences are respected in the future. If an individual asks for their Personal Data to be removed or erased then that must be done without undue delay.

17. Sharing Personal Data

Generally, FF is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. Representatives of FF may only share the Personal Data we hold with another employee, agent or representative of FF or any third party if the recipient has a job-related need to know the information and the transfer complies with any cross-border transfer restrictions.

Personal Data may only be shared with third parties (such as FF's business partners and IT support and other service providers) if:

(a) They have a need to know the information for the purposes of providing contracted services;

(b) Sharing the Personal Data complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;

(c) The third party has agreed to comply with the required data security policies and procedures and put adequate security measures in place;

(d) The transfer complies with any applicable cross border transfer restrictions; and

(e) A fully executed written contract that contains GDPR-approved third party clauses that has been obtained.