DATA PROTECTION POLICY

1. Principles and Policy

Future Focus Ltd (FFL) recognizes and upholds the importance of the correct and lawful treatment of personal data in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679 as complemented by the Maltese legislation – the Data Protection Act (Cap 586 of the Laws of Malta) and subsidiary legislation implemented under Chapter 586.

The objectives of this Data Protection Policy are:

i. To coordinate the information security and data handling procedures;
ii. To promote confidence in our information security and data handling procedures;
iii. To comply with relevant Eu and Maltese legislation and
iv. To provide a benchmark for employees on information security, confidentiality and data protection issues.

Objectives will be achieved by:

i. Implementing appropriate information handling policies and procedures for employees to follow and refer to; and
ii. Regular monitoring of the effectiveness of information handling policies and procedures to make amendments and additions as necessary from time to time.

2. Defining terms

For the purposes of this Data Protection Policy, the following terms shall have the following meanings:

"data" means information stored or processed by a computer and information recorded as part of a relevant filing system (which includes paper-based filing systems, card indexes and other non-electronic collections of data which are structured either by reference to individuals or so that information about an individual is easily accessible);

"personal data" means data about a living person who can be identified by that data;

"processing" means any operation performed on personal data, whether or not by automated means, such as obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, disseminating, aligning, combining, blocking, erasing or destroying data;

"controller" means a natural or legal person, public authority, agency or other body which, alone or jointly, determines the purposes and means of the processing of personal data;

"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"data subject" means a person who is the subject of personal data;

"sensitive personal data" means personal data relating to physical or mental health, religious or philosophical beliefs, and membership of a Trade Union, political opinions, race or ethnic origin, information about sex life, criminal convictions or allegations of criminal conduct;

"data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Scope and application of policy for Future Focus Ltd (FFL)

Whilst the GDPR applies EU wide, in addition, the DPA and related subsidiary legislation apply to:

i. The processing of personal data of FFL data subjects by the controller or processor as established in Malta, regardless where the processing takes place;
ii. The processing of personal data of FFL data subjects who are in Malta by a controller or processor not established in the EU, and where processing activities are related to
    a) The offering of tuition, irrespective of whether a payment by the data subject situated in Malta is required or not
    b) The monitoring of behavior of FFL data subjects insofar as the activity takes place in Malta
iii. The processing of personal data of FFL data subjects by a controller not established

4. Key Principles

Personal data is processed lawfully, fairly and in a transparent manner. Controllers provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Personal data is only collected for specified, explicit and legitimate purposes and is not further processed in a manner that is incompatible with these purposes. At FFL, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed. FFL only processes the personal data that it actually needs to process in order to achieve its processing purposes.

All personal data is kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

5. Control of Personal Data

FFL has a duty to keep registration up to date. Personal data that FFL keeps will not be disclosed under the Freedom of Information Act. FFL suppliers and stakeholders are told that Future Focus may be obliged under the Freedom of Information act to disclose certain information, so that they can make a decision whether to work with us at the onset of their services.

FFL is the data controller of all personal data held and processed on its behalf. The relevant person within the Company monitors the use and deletion of data and ensure that staff follows this policy of data protection. Information is kept in line with our data retention guidelines. All employees are responsible for ensuring that information is not kept for longer the necessary, and that the retention period complies with any legal and/or contractual requirements. When a record containing personal data is to be disposed of, paper documentation is to be permanently destroyed by shredding or incinerating and computer equipment or media is to have all personal data completely destroyed by reformatting and/or overwriting.

All employees are committed to information security and management, whereby FFL provides clear directions on responsibilities and procedures. Internal and remote access to computerised information and host application software is controlled by appropriate levels of password, granted to staff on a “need to know” basis, with authorisation from the relevant line Manager. Security of computer information is provided by automated backup routines, run daily on all sites and configured according to professional best practice.

Access to our computer systems is restricted. It is controlled by passwords. When an employee logs into the computer system using a password, a record of the activities of that employee is automatically generated. Passwords are kept secure, and the computer system prompts a change of password every 40 days. Where an employee thinks that his/her password may have been disclosed, this must be reported immediately for a new password to be issued.

The Chief Executive supports staff to ensure the following for information resources:

i. That personal data is readily accessible to authorised individuals;
ii. That plans and procedures are in place for the necessary long term archiving of specific record types for purposes of access;
iii. That clear guidelines are established for disclosure to and consultation by legitimately interested parties of personal information stored on paper or computerised media; and
iv. That procedures are put in place for identification and removal of inappropriate or unnecessary personal data stored on any Future Focus information system.

FFL is committed to maintaining high standards of security and confidentiality for information in our custody and control. Such information includes business information, trade secrets, know-how and personal data relating to customers and clients, our own employees and third-party company representatives.

6. Monitoring use of company IT

All employees are responsible for reporting any issues with IT computer systems or with security to the Chief Executive. Use of FFL computer systems is for Company business purposes only.

Use of FFL IT facilities by employees, is monitored to check compliance with this policy. Breach thereof is a disciplinary offence and could result in disciplinary action by FFL. Any employee, contractor or subcontractor who becomes aware of a data security breach shall immediately notify the known circumstances to Chief Executive.

7. Data Protection Training

Training is available to those who need it. Staff is informed of their duty under the Data Protection Policy and are expected to comply with the rules laid down therein. There will be many purposes for collecting personal data, and at each point of collection it must be made clear to the person giving the information that FFL will hold the information only for specific purposes.

In general, the following declaration is used on forms, on the website and in scripts where personal data is to be collected as part of the process data, hence, “The information supplied on this form will be used to keep you informed of community related matters by telling you about publications, conferences and seminars in relation to funding projects. We would also like to contact you by letter, email or telephone to advise you of these events. If you would like to be kept informed please tick here []. Future Focus do not share their mailing lists with other organisations unless we advise you of it at the time of collecting your personal details”.

8. The obligation when using data processors

The obligation for appropriate technical and organisational security measures for personal data applies when information is passed from Future Focus (the “data controller”) to an outsource service provider who will process it on its behalf (the “data processor”). When the processing of personal data is outsourced, data controllers take steps to ensure the

reliability of their data processors both in the selection criteria for choosing a service provider and in subsequent monitoring of the provider's performance.

In addition, the data controller will have a written contract with its data processor(s) which commit the data processor to act only on the instructions of the data controller and to adhere to the requirements of this policy when processing personal data on behalf of the data controller.

9. Requests for Information by Data Subjects

All individuals who are the subject of personal data are entitled to:

- ask what information we hold about them and why;
- ask how to gain access to it;
- be informed how to keep it up to date;
- have inaccurate personal data corrected or removed;
- prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else;
- require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance; and
- be informed what we are doing to comply with our obligations under the Data Protection Malta.

Future Focus will usually provide this information for free depending on the ease of accessibility. Personal information is only released to the individual to whom it relates. When a request for information is received, care is taken to ensure that the individual requesting information is doing so legitimately.

10. Requests for Information by Public Bodies

Future Focus acknowledges that public bodies such as government departments are subject to the requirements of the Freedom of Information Act 2000 and the Environmental Information Regulations. Future Focus will:

- assist and cooperate with any public body to enable it to comply with its Information disclosure requirements;
- transfer to the relevant public body any Request for Information made under the FOIA that it receives as soon as practicable and in any event within two working days of receiving a Request for Information;
- provide the public body with a copy of all Information in its possession or power in the form requested within five working days of the public body requesting the Information;
- provide all necessary assistance as reasonably requested by the public body to enable it to respond to a Request for Information within the time for compliance set out in Section 10 of the FOIA or Regulation 5 of the Environmental Information Regulations, this is currently 20 days; and
- not respond directly to a Request for Information unless expressly requested to do so by the relevant public body.

The public body shall be responsible for determining at its absolute discretion whether any Information is exempt from disclosure under the FOIA or the Environmental Information Regulations.

Future Focus acknowledges that public bodies may, under the FOIA or the Environmental Information Regulations, be obliged to disclose Information:

- without consulting with Future Focus; or

- following consultation with Future Focus and having taken its views into account.

All Future Focus staff, consultants and contractors responsible for procuring and/or creating any new information systems or modifying existing systems will be responsible for ensuring that those systems will comply with Future Focus's Data Protection Policy and Procedures.

Policy review date: July 2020