(NAME OF SERVICE)

GENERAL DATA PROTECTION REGULATION POLICY
GDPR-02

Title: COMPLIANCE WITH GDPR (POLICY)

1.0 INTRODUCTION

1.1 The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union.

1.2 ~~The Regulations cover both written and computerised information and the individual's right to see such records. It is important to note that the Regulations also cover records relating to staff and volunteers.~~

1.3 The Regulations also cover personal information in relation to people who use our Services. Personal information is defined in GDPR as "any information relating to an identified or identifiable natural person ("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.

1.4 ~~The General Data Protection Regulations requires our Service as a controller of data subject's personal information, to register with the Information Commissioners office.~~

1.5 This Data Protection Policy has been designed to lay the essential groundwork within our Service for compliance with data protection law (currently the Data Protection Act 1998 and, as of 25 May 2018, the GDPR).

2.0 POLICY

2.1 ~~This privacy policy is designed to ensure that we comply with the legal requirements of the General Data Protection Regulation (GDPR) and protect the personal information of people who use our services, staff and volunteers (data subjects~~).

3.0 PRINCIPLES OF GENERAL DATA PROTECTION REGULATION

3.1 We are committed to the Principles of Article 5 of the GDPR which requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

3.2 ~~The data controller shall be responsible for, and be able to demonstrate, compliance to the GDPR principles.~~

4.0 STEPS TOWARDS IMPLEMENTATION OF OUR GDPR POLICY

4.1 Establishing a lawful basis

Under EU data protection law, there must be a lawful basis for all processing of personal data (unless an exemption or derogation applies).

- The data subject has given consent;
- Processing is necessary for the performance of a contract;
- Processing is necessary for compliance with a legal obligation;
- Processing is necessary in order to protect the vital interests of the data subject;
- Processing is necessary for the performance of a task carried out in the public interest;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller.

4.2 PROCESSED FAIRLY AND LAWFULLY

4.2.1 ~~We will record and process fairly and lawfully information in language that is appropriate to the needs of our Service Users, staff and volunteers;~~

4.2.2 We will ensure that all organisations who provide services for us are informed about when and why we need to hold data about them;

4.2.3 We will inform all parties of any non-obvious uses of data being held by our Service;

4.2.4 ~~We will ensure that all Service Users, staff and volunteers are made aware of aware of the personal information we hold on them.~~

5.0 OBTAINED FOR SPECIFIED AND LAWFUL PURPOSES.

5.1 ~~There will always be a specific reason or purpose for collecting data on those who use our Service, volunteers or those employed by us.~~

5.2 We will ensure that all data is specifically collected for the sole purpose it is intended.

6.0 ADEQUATE, RELEVANT AND NOT EXCESSIVE

6.1 We will collect just the right amount of information from those who use our Service or provide a service (no more and no less), and only for the specific purpose intended.

7.0 ACCURATE AND UP TO DATE DATA

7.1 The Service will ensure that all personal data collected, processed, and held is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

7.2 ~~The accuracy of personal data shall be checked when it is collected and at regular~~ **~~intervals or insert interval~~**~~. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.~~

7.3 We will carry out an audit of our data processing at least annually to ensure it is accurate and complies with GDPR.

8.0 DATA RETENTION

(See Retention of Personal Data Policy Ref: GDPR 29).

8.1 The Service 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.

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

8.3 ~~We will specify the retention period of personal data records and carry out disposal of data which exceed the retention period in accordance with data protection. When any personal data has served its purpose, it will be disposed of accordingly.~~

9.0 CONSENT

(See Obtaining Consent Policy Ref: GDPR-07).

10.0 RIGHTS OF PEOPLE WHO PROVIDE PERSONAL INFORMATION

10.1 Rights of data subjects

10.1.1 ~~We are obliged to give effect to the rights of data subjects under EU data protection law.~~

10.2 Transparent communication

10.2.1 In order to ensure that personal data are processed fairly, EU data protection law obliges us to communicate transparently with data subjects regarding the processing of their personal data.

10.3 Identifying data subjects

10.3.1 ~~We must protect the rights of data subjects where third parties might attempt to exercise a data subject's rights without proper authorisation to do so. We must ask data subjects to provide proof of their identity before giving effect to their rights.~~

10.4 Right to basic information-keeping data subjects informed

10.4.1 In order to comply with a core principle of EU data protection law we will ensure that data subjects are provided with information concerning the purposes for which their personal data will be processed.

10.4.2 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- If the personal data is used to communicate with the data subject, when the first communication is made; or
- If the personal data is to be transferred to another party, before that transfer is made; or
- As soon as reasonably possible and in any event not more than one month after the personal data is obtained.

10.4.3 ~~We shall provide the following to every data subject:~~

- ~~Details of the Service including, but not limited to, the identity of the person responsible for data protection;~~
- ~~The purpose(s) for which the personal data is being collected and will be processed (as detailed in GDPR-10 Informing Service Users about GDPR) and the legal basis justifying that collection and processing;~~

- Where applicable, the legitimate interests upon which the Service is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- ~~Where the personal data is to be transferred to one or more third parties, details of those parties;~~
- ~~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;~~
- Details of data retention;
- Details of the data subject's rights under the GDPR;
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- 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; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

10.5 Right of access

10.5.1 In order to allow data subjects to enforce their data protection rights, we will enable data subjects to access their personal data.

10.5.2 ~~Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which~~

10.5.3 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.

10.5.4 All SARs received shall be handled by the person with responsibility for data protection.

10.5.5 ~~We will not charge a fee for the handling of normal SARs. The Service 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.~~

10.6 Data subjects have the right to obtain the following:

- Confirmation of whether, and where, the controller is processing their personal data;
- Information about the purposes of the processing;

- Information about the categories of data being processed;
- Information about the categories of recipients with whom the data may be shared;
- Information about the period for which the data will be stored (or the criteria used to determine that period);
- Information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;
- Information about the existence of the right to complain to the ICO;
- Where the data were not collected from the data subject, information as to the source of the data; and
- Information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects.

Additionally, we will make data subjects aware of how they can request a copy of the personal data being processed.

10.7 Right to erasure (the "right to be forgotten")

10.7.1 ~~Data subjects are entitled to require a controller to delete their personal data if the continued processing of those data is not justified~~

10.7.2 Data subjects have the right to erasure of personal data (the "right to be forgotten") if:

- The data are no longer needed for their original purpose (and no new lawful purpose exists);
- The lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists;
- The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;
- ~~The data have been processed unlawfully; or~~
- ~~Erasure is necessary for compliance with EU law or the national law of the relevant Member State.~~
- 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).

10.8 Right to portability

10.8.1 We must ensure that the data subjects Service Users, staff and volunteers personal data can be provided to them in a structured, commonly used and machine-readable form, so that software can extract specific elements of the data. This will enable other organisations to use the data.

10.8.2 ~~Where employee data subjects have given their consent to the Service to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Service and the employee data subject, employee data subjects have the right, under the GDPR, to receive a copy of their~~ personal data and to use it for other purposes (namely transmitting it to other data controllers).

10.8.3 ~~Where technically feasible, if requested by an employee data subject, personal data shall be sent directly to the required data controller.~~

10.9 Right to object

10.9.1 We have an obligation to inform data subjects of their rights to object to the processing of their personal data. This must be communicated to the data subject no later than the time of the first communication with the data subject. This information should be provided clearly and separately from any other information provided to the data subject.

10.9.2 ~~Where a data subject objects to the Services processing their personal data based on its legitimate interests, the Service shall cease such processing immediately, unless it can be demonstrated that the Services 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.~~

11.0 RECTIFICATION OF PERSONAL INFORMATION

11.1 a) Data subjects have the right to require the Service to rectify any of their personal data that is inaccurate or incomplete.

b) The Service shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Service 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.

c) 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.

12.0 RESTRICTION OF PERSONAL DATA PROCESSING

12.1 Data subjects may request that the Service ceases processing the personal data it holds about them. If a data subject makes such a request, the Service 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.

12.2 ~~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).~~

13.0 DISPOSAL OF PERSONAL DATA

13.1 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.

14.0 TECHNICAL AND SECURITY MEASURES

(See Security of Personal Data Policy Ref: GDPR-15).

15.0 DATA BREACHES

(See Information Governance Policy Ref: GDPR-11).

16.0 INFORMATION RISKS

16.1 The manager will ensure that risk assessments are carried out on the protection and back up storage of data subject's personal information. In particular what measures will be put in place to protect data subjects from loss of their information.

17.0 DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

17.1 The manager will carry out Data Protection Impact Assessments for any and all new projects, and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

17.2 Data Protection Impact Assessments should be overseen by the person responsible for data protection or Data Protection Officer and shall address the following:

- ~~The type(s) of personal data that will be collected, held, and processed;~~
- ~~The purpose(s) for which personal data is to be used;~~
- ~~The Service's objectives;~~
- ~~How personal data is to be used;~~
- ~~The parties (internal and/or external) who are to be consulted;~~
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Service; and
- Proposed measures to minimise and handle identified risks.

17.3 Where applicable we will use the ICO Code of Practice on Impact Assessments.

18.0 EMPLOYMENT CONTRACTS

18.1 The manager must ensure that every employee's contract of employment informs the employee, in broad terms, how their personal data will be used, and obtain their agreement to the collection, processing, and holding of their personal data for such use.

19.0 SECURE PROCESSING

19.1 The Service 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.

20.0 ACCOUNTABILITY AND RECORD KEEPING

20.1 The manager will ensure that the Service complies with the legal requirements of General Data Protection Regulations. The Service we will carry out regular monitoring and auditing of our data protection policies and regularly review the effectiveness of data handling and security controls.

20.2 ~~The nominated person (insert name) responsible for data protection shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Service's other data protection-related policies, and with the GDPR and other applicable data protection legislation.~~

20.3 The Service is responsible for keeping:

- Name and details of the Service, person responsible for data protection and any applicable third-party data processors;
- The purposes for which the Service collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Service, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Service; and
- Detailed descriptions of all technical and organisational measures taken by the Service to ensure the security of personal data.

21.0 STAFF TRAINING

(See Staff Training Policy Ref: GDPR 16).

DISCLAIMER

(NAME OF SERVICE)

GENERAL DATA PROTECTION REGULATION POLICY
GDPR-02

The Bettal General Data Protection Compliance Tool has been produced on the basis of best practice with particular reference to the guidance provided by the Information Commissioners Office.

As Bettal Quality Consultancy has no control over how these documents will be used to process personal data we will not be liable for any damages, losses or causes of action of any nature arising from any use of any of the documents or the provision of these documents."