DATA PROTECTION POLICY

1. INTRODUCTION

Everyone has rights with regard to how their personal information is handled. During the course of the Organisation's activities it will collect, store and process personal information, and recognises the need to treat it in an appropriate and lawful manner.

All information processed is subject to certain legal safeguards specified in the General Data Protection Regulations (GDPR). The Act imposes restrictions on how the Organisation may use that information.

Any breach of this policy may result in an investigation which may in turn lead to a disciplinary hearing. Any serious breaches will be reported to the ICO in line with the legislation.

Please read this document together with the Privacy Notice.

2. STATUS

This policy sets out the Organisation's 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 information.

The Data Protection Compliance Officer is responsible for ensuring compliance with the Act. Details of who is the current Data Protection Compliance Officer can be found in Appendix 1. Any questions or concerns about the operation should be referred in the first instance to the Data Protection Compliance Officer.

If you consider that the Organisation's provisions for complying with the Act have not been followed in respect of personal data about yourself or others you should raise the matter with the Data Protection Compliance Officer.

This policy does not form part of your contract of employment or that of any other person employed by Strings of Life and may be amended at any time.

3. DEFINITION OF DATA PROTECTION TERMS

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

Data subjects for the purpose of this policy include all living individuals about whom the Organisation holds 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.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in the Organisation's 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).

Data controllers are the people/organisations who determine the purposes and the manner in which any personal data is processed. The Organisation is the data controller of all personal data used in its business for its own commercial purposes and has a responsibility to establish practices and policies in line with the Act.

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

Data processors include any person who processes personal data on behalf of a data controller. Data controllers are excluded from this definition but it could include suppliers that handle personal data on the Organisation's behalf.

Processing is any activity that involves use of the 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.

Sensitive personal data includes information 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 life, 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 express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

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

- processed fairly and lawfully, and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about;
- kept securely;

- not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

The Act 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. You have a right to be told who the data controller is, and in this case it is Strings of Life. You have a right to be told who the data controller's representative is and in this case this is the Data Protection Compliance Officer, details of whom can be found in Appendix 1. You also have a right to be told the purpose for which the data is to be processed by the Organisation, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, requirements that the data subject has consented to the processing, the processing is necessary for the legitimate interest of the data controller, the performance of the employment contract, compliance with a legal obligation, vital interests or a public interest. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6. PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must 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, you, as the data subject, must be informed of the new purpose before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should 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 should not be collected in the first place.

8. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should 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 should be destroyed.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from the Organisation's systems when it is no longer required.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. You as a data subject has a right to:

- The right to transparency
- The right to information and access to personal data
- The right to rectification
- The right to erasure (to be forgotten)
- The right to restriction of processing
- The right to data portability
- The right to object to processing
- Rights in relation to automated decision making

11. DATA SECURITY

The Organisation must 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. You as a data subject may apply to the courts for compensation if you have suffered damage from such a loss.

The Act requires the Organisation 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 the third party agrees to comply with those procedures and policies, or if they put in place adequate measures themselves.

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

- confidentiality means that only people who are authorised to use the data can access it;
- integrity means that personal data should be accurate and suitable for the purpose for which it is processed;

- 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 the Organisation's central drive of individual PCs or laptops.

Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported;
- 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);
- Methods of disposal. Paper documents should be shredded. Floppy disks, CD-ROMs and pen sticks should be physically destroyed when they are no longer required;
- 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.

12. DEALING WITH SUBJECT ACCESS REQUESTS

If you want access to information that the Organisation holds about you then the request must be made in writing.

If you receive a written request you should forward it to the points of contact listed in Appendix 1 Officer immediately.

There will be no charge for the service and a response will be given with 1 month.

Data subjects have the right to be forgotten where personal data is no longer necessary for the purposes for which it was collected, this includes any data issued to a third party, if you wish to be forgotten then please make your request in writing to the Trustee.

13. PROVIDING INFORMATION OVER THE PHONE

If you as part of your job in the Organisation deal with telephone enquiries it is your duty to be careful about disclosing any personal information held by the Organisation. In particular you should:

- check the caller’s identity to make sure that information is only given to a person who is entitled to it;
- suggest that the caller put their request in writing if they are not sure about the caller’s identity and where their identity cannot be checked;
- refer to the points of contact listed in appendix 1 for assistance in difficult situations. No-one should be bullied into disclosing personal information.

14. Reporting a breach

If you become aware of a breach of the regulations then you must in the first instance report the full details of the breach to the points of contact listed in Appendix 1;

- The Organisation will then report the breach if necessary to the ICO;
- All Data subjects will be informed of any breaches.

APPENDIX 1

Points of contact for Data Protection issues are:

Christina Lam, Data Protection Compliance Officer

Who can be contacted by:

Email: christina@lcgcsol.onmicrosoft.com