Time Out Data Security Policy – Looking After the Personal Data of Others

Throughout this document, Time Out Group (Stratford-upon-Avon) Limited and the charitable activities carried on by it as The Time Out Group are referred to as "Timeout" or "the Charity"

1. Policy Statement

Timeout needs to gather and use data about individuals including its service users and their families, donors and its staff in order to meet its charitable objectives as well as possible. Timeout is committed to ensuring the security of data that it receives, collects, creates and uses and adheres to the principles of the General Data Protection Regulation effective 25th May 2018.

This policy sets out the **security procedures** and describes the **internal controls** to be followed by its staff to protect data relating to all individuals that Timeout has contact with. It also describes the procedure to be followed if an individual makes any request regarding the personal data held by Timeout. Finally in the appendices of this policy there is further information in the form of privacy statements applicable to individuals working or potentially working for the Charity or customers in the form of service users and their families.

2. Scope of Policy

The security procedures and internal controls described in this policy are designed to protect data relating to any individual Timeout has contact with which includes the following individuals but may not be an exhaustive list as Timeout makes new contacts on an on-going basis:

- Service Users and their families
- Donors
- Suppliers – for example, premises, insurance, payroll, DBS check providers, accountant
- Other organisation contacts – for example, bank, HMRC, governance bodies
- Employees – both permanent and temporary
- Voluntary Workers/Work Experience Students/Agency Workers or anyone else performing work for Timeout.

The security procedures and internal controls are to be adhered to by all employees, both permanent and temporary and anyone else performing work for the Charity.

3. Definitions of Data

- Personal data – is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data including collecting, storing, amending, disclosing or destroying it.

- Special categories of personal data – means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric or genetic data.

- Criminal records data – means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

4. Responsibility for Data Protection

Timeout has appointed the Group Leader as the person responsible for data protection compliance within the organisation. He/she can be contacted at timeoutgroup@hotmail.com with any questions about this or any other policies relating to the protection of personal data.

5. Data Protection Principles

Timeout processes personal data in accordance with the following principles:

- Processing personal data lawfully, fairly and in a transparent manner.
- Collecting personal data only for specified, explicit and legitimate purposes.
- Processing personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeping accurate personal data and taking all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Keeping personal data only for the period necessary for processing.
- Adopting appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- Communicating to individuals the reasons for processing their personal data.
- Assessing the reasons for processing data and ensuring these are not over-ridden by the rights and freedoms of individuals.
- Where Timeout engages third parties to process personal data on its behalf, such parties do so, on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and other measures to ensure the security of data.

6. Security Procedures and Internal Controls

All staff are required to follow the procedures and controls set out below to ensure Timeout is able to comply fully with the protection of personal data.

Any breach of these rules will be regarded very seriously and be handled in accordance with the procedures described in Section 8 of this document. It is therefore very important for all staff to have a clear understanding of Timeout's requirements and staff are encouraged to immediately raise any queries at all about implementing these procedures and controls with the Group Leader or in their absence the person with overall responsibility for Data Protection, the Secretary.

a. Confidentiality:

- All staff are required to comply with the confidentiality clause in their employment contract or in the case of non-employed staff the terms of their working agreement with Timeout.
- Data must not be shared externally unless this is authorised by Timeout.
- Data must not be shared internally with unauthorised colleagues.
- The above includes verbal disclosure of personal data as well as data being shared in paper or electronic format.

- Failure to comply with confidentiality requirements will be treated very seriously as a breach of the contract with Timeout. Please see section 8 below for further detail on this.

b. The authority to collect, process, use, maintain, keep, and destroy data:

- All staff with access to data must legitimately require it to perform their duties. Authorisation to collect, process, use, maintain, keep and destroy data is described within a variety of documents that detail an individual's work duties, including job descriptions, other agreed contractual arrangements, standard operating procedures, quality procedures and may also be provided in the form of verbal instructions from the Group/Acting Group Leader. Specified procedures are in place for dealing with especially sensitive personal data and must be followed at all times – see Appendices to this Policy
- Data must not be shared with internal work colleagues unless their duties require them also to have access and in such circumstances the data will only be shared to the extent necessary.
- Any other data in the possession of staff must immediately be advised to the Group Leader for instructions as to how this data should be treated including its immediate and secure disposal.
- Data must be held in as few a places as possible and staff should not create unnecessary additional copies unless there is a legitimate reason to have copies. Staff must regularly review data in their possession and ensure they do not have unnecessary duplicate sources of information.

c. All data to be accurate and up to date

- All staff should do their utmost to ensure that the data they hold for work purposes is accurate and up to date. Any concerns that staff have about this not being the case must be advised to the Group Leader for instructions as to how this data should be treated including its immediate updating or secure disposal.
- Data should be regularly reviewed and updated if found to be out of date with old data being securely disposed.

d. Paper data to be held securely

- Paper data should be kept in a locked drawer or filing cabinet.
- Paper data should not be left unattended and should be kept in a locked drawer or filing cabinet until it is being worked on.
- Data which is no longer being used for current processing or does not need to be held as a historical record should be shredded.

e. Electronic data to be held securely

- Passwords
    i. Staff should protect access to personal data through the use of strong passwords.
    ii. Staff must ensure that they protect the confidentiality of the data if they access it electronically in a non-confidential environment and ensure that it cannot be viewed by anyone not authorised to view or use it, including members of the public who may be able to view information displayed or being worked on. Computers left unattended whilst data is being worked on should be locked to prevent viewing and access.
- Back Up
    iii. Data should be backed up frequently.
    iv. All servers and computers should be protected by approved security and firewall.

- Removable Media
    v. If data is stored on removable media (eg. memory stick/disc/card) this should be locked away securely when not in use and should be password protected.

f. Building Security

Controls are in place to protect personal data from unauthorised access when Timeout staff are located at its operating base.

- The building security measures in place to protect the safety of service users also help Timeout protect its personal data. Staff are provided with a passcode to enter the front door to the building. This passcode must be kept confidential and staff must advise the Group Leader when they become aware of this confidentiality being breached.
- Staff are also required to approach individuals they do not recognise as authorised visitors to ensure they have signed in and are under the supervision of a work colleague. .

g. Staff Training

- All staff are provided with a briefing on the requirements regarding data protection as part of their induction process and asked to demonstrate their understanding of these in regards to their work activities
- Staff should request help and advice from the Group Leader if they are uncertain about any aspect of data protection.
- Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

h. Monitoring

- Right of Search – Should Timeout suspect that there is any unauthorised data being physically removed from Timeout premises or downloaded onto removable or personal devices, whether this be personal data or any other Timeout data, it is entitled to carry out a search of any vehicle, bag or other container in an employee's possession. In cases where the individual is not employed by Timeout, the police may be called on suspicion of theft of any data and also upon discovery of any data theft by an employee.

7. <u>Data Protection and Subject Access Rights of Individuals</u>

As a data subject, individuals have a number of rights in relation to their personal data.

a. Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, Timeout will tell him/her:

- Whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of data if it is not collected from the individual;
- To whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area and the safeguards that apply to such transfers:
- For how long his/her personal data is stored (or how that period is decided)

- His/her rights to rectification or erasure of data, or to restrict or object to processing; and
  His/her right to complain to the Information Commissioner if he/she thinks Timeout has failed to comply with his/her data protection rights
- Timeout does not at present carry out automated decision-making.

Timeout will also provide the individual with a copy of the personal data undergoing processing. If the individual wants additional copies, Timeout will charge a fee, which will be based on the administrative cost of providing such copies.

b. Making A Subject Access Request

- The individual should send the request in writing by email to the Group Leader.
- The request will normally be responded to within a period of 1 month from the date it is received and at the latest within 3 months. Individuals will be advised within one month if the request will take longer than one month to respond to.
- If the subject access request is manifestly unfound or excessive, Timeout is not obliged to comply with it. Alternatively Timeout can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfound and/or excessive where it repeats a request which has already been responded to. Timeout will notify the individual if this is the case and whether or not it will respond to it.

c. Other Rights

Individuals have a number of other rights in relation to their personal data. They can require Timeout to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests over-ride Timeout's legitimate grounds for processing data (where Timeout relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful and ;
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests over-ride the Company's legitimate grounds for processing data.
- To ask Timeout to take any of these steps, the individual should send the request to the Timeout Group Leader.

8. Breach of the Security Procedures and Internal Controls

- Disciplinary sanctions for employees; Failure to observe the data security requirements may amount to a disciplinary offence, which will be dealt with under Timeout's disciplinary procedure. Significant or deliberate breaches of this policy such as accessing employee or service user data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

- Sanctions for 3rd parties (all those not employed and not subject to disciplinary proceedings): Any breach of data security arrangements with 3rd parties will be vigorously investigated by Timeout, and could lead to the cancellation of contractual agreements and the pursuit of legal action for any damages caused by a breach.

- If Timeout discovers that there has been a breach of HR related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Timeout will record all data breaches regardless of their effect.

- If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

- Staff are required to immediately report data breaches of which they become aware to the Group Leader/Acting Group Leader or a Member of the Board of Trustees in their absence.

APPENDICES

Appendix 1 **Privacy Statement – The privacy of individuals who perform work for Timeout**

Appendix 2 **Privacy Statement – The privacy of service users who attend Timeout activities**

Appendix 3 **Privacy Statement – The privacy of individuals who support and donate to Timeout**

Appendix 1

Privacy Statement – The privacy of individuals who perform work for Timeout

Timeout collects and processes personal data relating to its staff to manage their employment and other working arrangements. Timeout is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

a. **What information does Timeout collect?**

Timeout collects and processes a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number, date of birth and gender; the terms and conditions of your employment;
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with Timeout;
- Information about your remuneration
- Details of your bank account and national insurance number;
- Information about your marital status, next of kin, dependants and emergency contacts;
- Information about your nationality and entitlement to work in the UK;
- Information about your criminal record (if you have one);
- Details of your days of work and working hours and attendance at work;
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- Assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- Information about medical or health conditions, including whether or not you have a disability for which the Company needs to make reasonable adjustments;

Timeout collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

Timeout seeks information from third parties with your consent only such as for references in the employment offer process and for DBS checks required for working with our service users.

Data is stored in a range of different places, including in your personnel paper file, in the Treasurer's paper and/or personal computer files where necessary for payment of salaries and expenses, and in the electronic records of our payroll provider.

b. **Why does Timeout process personal data?**

Timeout needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer any other contractual entitlements.

In some cases, Timeout needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, Timeout has a legitimate interest in processing personal data before, during and after the end of the employment relationship.

Processing employee data allows Timeout to:

- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- Operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that Timeout complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- Ensure effective general HR and business administration;
- Run recruitment processes;
- Provide references on request for current or former employees;
- Contribute to the external audit of Timeout's financial accounts;.
- Respond to and defend against legal claims; and
- Maintain and promote equality in the workplace.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations such as those in relation to employees with disabilities and for health and safety purposes.

Information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings is sought in order to carry out a DBS check required by law for all staff in contact with our service users.

c. **Who has access to data?**

Your information will be accessed by the Time Out Secretary and will be shared internally with the Trustee Board of Directors and the Group Leader and Acting Group Leader where it is necessary to enable them to perform aspects of their duties.

Timeout may also share your data with third parties in the context of a transfer of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

Timeout currently shares your data with third parties that process data on its behalf in connection with the provision of a payroll service and a DBS checking service. It may also share data with an Occupational Health Service provider if this is necessary. Data is provided to meet any statutory or government body request.

The Charity will not transfer your data to countries outside the European Economic Area.

d. **How does Timeout protect data?**

Timeout takes the security of your data seriously. Timeout has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where Timeout engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

e. **For how long does Timeout keep data?**

The Company will hold your personal data for the duration of your working arrangement. After the end of the working relationship Timeout will hold all data necessary to respond to tax, reference or other statutory enquiries for 7 years. All other data held for staff

will be held for 3 months (unless there are exceptional circumstances where, for example there is a dispute in which case data may be held until no longer considered necessary) .

f. **Your rights**

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request;
- Require Timeout to change incorrect or incomplete data;
- Require Timeout to delete or stop processing your data in certain circumstances, for example where the data is no longer necessary for the purposes of processing;
- Object to the processing of your data where Timeout is not relying on its legitimate interests as the legal ground for processing; and
- Ask Timeout to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Timeout's legitimate grounds for processing data.
- If you would like to exercise any of these rights, please contact the Group Leader.
- If you believe that Timeout has not complied with your data protection rights, you can complain to the Information Commissioner.

g. **What if you do not provide personal data?**

You have some obligations under your employment contract to provide Timeout with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith.

You may also have to provide Timeout with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable Timeout to enter a contract of employment with you. If you do not provide other information, this will hinder Timeout's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Appendix 2

Privacy Statement – The privacy of service users who attend Timeout activities

Timeout collects and processes personal data relating to its service users to manage the service provided to them. Timeout is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

a. **What information does Timeout collect?**

Timeout collects and processes a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number, date of birth and gender;
- Information about your medical or health conditions, your disability diagnosis and support needs
- Any Statement of Special Educational Needs
- Family makeup,
- Professionals involved with you or your family

Timeout collects this information in a variety of ways. For example, through interviews and referral forms

Timeout seeks information from third parties with your verbal consent only such as school.

Data is stored in a range of different places, including in a lockable paper file or on a dedicated laptop computer, which is password protected

b. **Why does Timeout process personal data?**

Timeout needs to process data to protect Service Users, for example to enable us to prepare risk assessments
In some cases, Timeout needs to process data to ensure that it is complying with its legal obligations.

In other cases, Timeout has a legitimate interest in processing personal data before, during and after the end of the service user relationship.

Processing service user data allows Timeout to continue to operate its services in a safe, knowledgeable and effective way.

c. **Who has access to data?**

Your information will be accessed by the Group Leader/Acting Group Leader and staff where it is necessary to enable them to perform aspects of their duties.

Timeout may also share your data with third parties in the context of a transfer of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

Timeout does not currently share your data with any third parties

The Charity will not transfer your data to countries outside the European Economic Area.

d. **How does Timeout protect data?**

Timeout takes the security of your data seriously. Timeout has internal policies and controls in place to try to ensure that your data is accurate, is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its staff in the performance of their duties.

Where Timeout engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

e. **For how long does Timeout keep data?**

The Charity will hold your personal data for the duration of you using our service. After you no longer use our service Timeout will normally hold data for three years, or in exceptional circumstances for longer if in our opinion it is justified (for example where there has been a significant untoward incident for which an investigation is or may be ongoing).

f. **Your rights**

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request;
- Require Timeout to change incorrect or incomplete data;
- Require Timeout to delete or stop processing your data in certain circumstances, for example where the data is no longer necessary for the purposes of processing;
- Object to the processing of your data where Timeout is not relying on its legitimate interests as the legal ground for processing; and
- Ask Timeout to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Timeout's legitimate grounds for processing data.
- If you would like to exercise any of these rights, please contact the Group Leader.
- If you believe that Timeout has not complied with your data protection rights, you can complain to the Information Commissioner.

g. **What if you do not provide personal data?**

Certain information, such as family contact details, your health and care requirements must be provided to enable Timeout to provide you with our service.

Appendix 3

Privacy Statement – The privacy of individuals who support and donate to Timeout

Timeout collects and processes personal data relating to individuals who support and donate to it in order to pursue its legitimate interests of raising funds for its charitable activities. Timeout is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

h. **What information does Timeout collect?**

Timeout may collect and process a range of information about you. This may include:

- Your name, address and contact details, including email address and telephone number;
- Details of your bank account (this is necessary if you are a regular donor by Standing Order); and
- Whether or not you are a UK taxpayer (if you are eligible for Gift Aid)

Timeout collects this information from you in a variety of ways. For example, data is collected through your donating via our online donation process, or when you complete a physical Standing Order form and/or Gift Aid application form.

Timeout does not seek information from third parties but needs to submit your Standing Order form to your bank for processing.

Data is stored in a locked physical file by the Hon. Treasurer and will not be shared with any third party without your express permission.

i. **Why does Timeout process personal data?**

Timeout needs to process data as part of its legitimate interest to ensure that we understand who our benefactors are, to inform them about our activities, to ensure that they are appropriately thanked and that funds are properly credited to Timeout's bank account, and to claim Gift Aid if appropriate.

Processing donor data allows Timeout to:

- Maintain accurate and up-to-date records and contact details of its donors and benefactors;
- Maintain contact with supporters to update them on our activities and further opportunities to support us; and
- Contribute to the external audit of Timeout's financial accounts;.

j. **Who has access to data?**

Your information will be accessed by the Hon. Treasurer and will be shared internally with the Trustee Board of Directors and the Group Leader and Acting Group Leader where it is considered necessary or appropriate by the Board

Other than Her Majesty's Customs & Excise for the purposes of claiming Gift Aid if relevant, Timeout will not normally share your data with any third party, but may share your data with a government or regulatory body if necessary to meet a statutory or government body request, and in exceptional circumstances with third parties in the context of a transfer of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The Charity will not transfer your data to countries outside the European Economic Area.

k. **How does Timeout protect data?**

Timeout takes the security of your data seriously. Timeout has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its staff and Trustees in the performance of their duties.

l. **For how long does Timeout keep data?**

The Charity will hold your personal data for as long as we consider we have a legitimate interest in doing so. We define this as the period up to four years after your latest donation, or four years after you terminate your Standing Order. After this date Timeout will hold all data necessary to respond to tax, reference or other statutory enquiries for a further three years. All other data held for donors will be held for up to a further 3 months and then destroyed.

Your rights

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request;
- Require Timeout to change incorrect or incomplete data;
- Require Timeout to delete or stop processing your data in certain circumstances, for example where the data is no longer necessary for the purposes of processing;
- Object to the processing of your data where Timeout is not relying on its legitimate interests as the legal ground for processing; and
- Ask Timeout to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Timeout's legitimate grounds for processing data.
- If you would like to exercise any of these rights, please contact the Group Leader.
- If you believe that Timeout has not complied with your data protection rights, you can complain to the Information Commissioner.

m. **What if you do not provide personal data?**

You do not need to provide any data to Timeout in order to donate.

This policy was adopted by the committee on 27 November 2018

Signed……. Chair ……. Date