Privacy Policy

1. Introduction

Stoll is committed to ensuring the secure and safe management of data held in relation to customers, staff and other individuals. Stoll's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

Stoll needs to gather and use certain information about individuals. These can include customers (tenants, service users, donors etc.), employees and other individuals that Stoll has a relationship with. Stoll manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

2. Legislation

It is a legal requirement that Stoll process data correctly; Stoll must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

a) the General Data Protection Regulation (EU) 2016/679 ("the GDPR");
b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
c) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union

3. Data

3.1 Stoll holds a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by Stoll is detailed within the Fair Processing Notice at Appendix 2 hereto and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

3.1.1 "Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by Stoll.

3.1.2 Stoll also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Processing of Personal Data

4.1 Stoll is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 4.4 hereof);
- Processing is necessary for the performance of a contract between Stoll and the data subject or for entering into a contract with the data subject;
- Processing is necessary for Stoll's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of Stoll's official authority; or
- Processing is necessary for the purposes of legitimate interests.

4.2 Fair Processing Notice

4.2.1 Stoll has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held by Stoll. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The Fair Processing Notice at Appendix 1 sets out the Personal Data processed by Stoll and the basis for that Processing. This document is provided to all of Stoll's customers at the outset of processing their data

4.3 Employees

4.3.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by Stoll. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

4.3.2 A copy of any employee's Personal Data held by Stoll is available upon written request by that employee from Corporate Services.

4.4 Consent

Consent as a ground of processing will require to be used from time to time by Stoll when processing Personal Data. It should be used by Stoll where no other alternative ground for processing is available. In the event that Stoll requires to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant

consent form if willing to consent. Any consent to be obtained by Stoll must be for a specific and defined purpose (i.e. general consent cannot be sought).

Appendix 2 hereto details Stoll's Consent Form/s.

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that Stoll processes Special Category Personal Data or Sensitive Personal Data, Stoll must do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

5. Data Sharing

Stoll shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with Stoll's relevant policies and procedures. In order that Stoll can monitor compliance by these third parties with Data Protection laws, Stoll will require the third party organisations to enter in to an Agreement with Stoll governing the processing of data, security measures to be implemented and responsibility for breaches.

5.1 Personal data is from time to time shared amongst Stoll and third parties who require to process personal data that Stoll process as well. Both Stoll and the third party will be processing that data in their individual capacities as data controllers.

5.2 Where Stoll shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with Stoll in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

5.3 Data Processors

5.3.1 A data processor is a third party entity that processes personal data on behalf of Stoll, and are frequently engaged if certain of Stoll's work is outsourced (e.g. payroll, maintenance and repair works).

5.3.2 A data processor must comply with Data Protection laws. Stoll's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify Stoll if a data breach is suffered.

5.3.3 If a data processor wishes to sub-contact their processing, prior written consent of Stoll must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.3.4 Where Stoll contracts with a third party to process personal data held by Stoll, it shall require the third party to enter in to a Data Protection Addendum with Stoll in accordance with the terms of the model Data Protection Addendum set out in Appendix 4 to this Policy.

6. Data Storage and Security

All Personal Data held by Stoll must be stored securely, whether electronically or in paper format.

6.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with Stoll's storage provisions.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to Stoll's data processors or those with whom Stoll has entered in to a Data Sharing Agreement. If Personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. Breaches

A data breach can occur at any point when handling Personal Data and Stoll has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

7.1 Internal Reporting

7.1.1 Stoll takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

7.1.2 As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the DPO must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);

7.1.3 Stoll must seek to contain the breach by whatever means available;

7.1.4 The DPO must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with this clause 7;

7.1.5 Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

7.2 Reporting to the ICO

7.2.1 The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data Protection Officer ("DPO")

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by Stoll with Data Protection laws. Stoll has elected to appoint a Data Protection Officer whose details are noted in the Data Protection Policy and contained within the Fair Processing Notice at Appendix 3 hereto.

The DPO will be responsible for:

a) monitoring Stoll's compliance with Data Protection laws and this Policy;
b) co-operating with and serving as Stoll's contact for discussions with the ICO
c) reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

9. Data Subject Rights

9.1 Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by Stoll, whether in written or electronic form.

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to Stoll's processing of their data. These rights are notified to Stoll's tenants and other customers in Stoll's Fair Processing Notice.

9.3 Subject Access Requests

Data Subjects are permitted to view their data held by Stoll upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, Stoll must

respond to the Subject Access Request within one month of the date of receipt of the request. Stoll:

a) must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.
b) where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request, or
c) where Stoll does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

9.4 The Right to be Forgotten

9.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing to Stoll seeking that Stoll erase the data subject's Personal Data in its entirety.

9.4.2 Each request received by Stoll will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request.

9.5 The Right to Restrict or Object to Processing

9.5.1 A data subject may request that Stoll restrict its processing of the data subject's Personal Data, or object to the processing of that data.

9.5.2 In the event that any direct marketing is undertaken from time to time by Stoll, a data subject has an absolute right to object to processing of this nature by Stoll, and if Stoll receives a written request to cease processing for this purpose, then it must do so immediately.

9.5.3 Each request received by Stoll will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

10. Privacy Impact Assessments ("PIAs")

10.1 These are a means of assisting Stoll in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 Stoll shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

10.3 Stoll will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer ("DPO") will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

11. Archiving, Retention and Destruction of Data

Stoll cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. Stoll shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the table at Appendix 5 hereto.

12. List of Appendices

1. Fair Processing Notices
2. Consent Forms
3. Data Sharing Agreement
4. Data Processor Addendum
5. Retention Table

Policy Review Form

The form below is designed to ensure that all of Stoll's policies remain 'live' and also conforms to the high levels expected of Stoll around areas such as equal opportunities, user involvement and continuous improvement.

The lead on each policy should retain this form and keep it updated continuously in order to feed into the ongoing review process of all policies. When presenting a new or existing policy for sign off by the SMT or the Trustee Board the completed policy review form must be presented.

Policy:	**Privacy Policy**
Date of last review:	May 2018
Date of next review:	
Approval by residents obtained on:	N/A
Beneficiaries' comments feeding into review:	N/A
Approval by partners obtained on:	N/A
Approved by SMT on:	2nd May 2018
Staff comments feeding into review:	N/A
Equality impact assessment:	
Changes made following equality impact assessment:	
Approval by Trustee Sub-committee on:	11th May 2018