1. Introduction

COOL HARBOUR is committed to a policy of protecting the rights and privacy of individuals (including clients, staff and others) in accordance with the EU Regulation 2016/679 General Data Protection Regulation ("GDPR"), Data Protection Act 1988, Data Protection (Amendment) Act 2003. COOL HARBOUR needs, for purpose of providing professional services and products, to process personal data about individuals (clients, employees, and other individuals with whom it has dealings). To comply with the law, personal data must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

2. Individuals' Responsibilities

Any staff member of COOL HARBOUR who is involved in the collection, storage or processing of personal data has responsibilities under the legislation. Any staff member involved in the processing/storing of personal data should make sure:

- to obtain and process personal data fairly
- to keep such data only for explicit and lawful purposes
- to disclose such data only in ways compatible with these purposes
- to keep such data safe and secure
- to keep such data accurate, complete and up-to-date
- to ensure that such data are adequate, relevant and not excessive
- to retain such data for no longer than is necessary for the explicit purpose
- to give, on request, a copy of the data to the individual to whom they relate; such a request is known as a DATA ACCESS REQUEST

3. Individual Rights

The individuals for whom COOL HARBOUR stores personal data have the following rights:

- to have their personal data obtained and processed fairly, kept securely and not illegitimately disclosed to others
- to be informed of the identity of the Data Controller and of the purpose for which the information is held
- to get a copy of their personal data
- to have their personal data corrected or deleted if inaccurate

- to prevent their personal data from being used for certain purposes: for example, one might want to have the data blocked for research purposes where they are held for other purposes
- pursuant to Employment Rights, not to be forced to disclose information to a prospective employer. No one can force another person to make an access request, or reveal the results of an access request, as a condition of recruitment, employment or provision of a service. Where vetting for employment purposes is necessary, this can be facilitated where the individual gives consent to the data controller to release personal data to a third party.

It should be noted that under the Freedom of Information Act (1997 and 2003) records containing personal information may be released to a third party, where the public interest so requires.

Each of the above rights are supported internally by policies & procedures that all the required action to be taken within timescales stated in the GDPR. For timescales please check Table 1 below

Data Subject Request	Timescale
Right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
Right to Access	One month
Right to Rectification	One month
Right to Erasure	Without undue delay
Right to restrict processing	Without undue delay
Right to data portability	One month
Right to object	On receipt of objection
Right to automated decision making and profiling	Not specified

Table 1 – Timescales for data subject requests

4. Consent

Unless it is necessary for a reason allowable in the GDPR, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be

obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge. If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

5. Principles of the Acts

COOL HARBOUR will administer its responsibilities under the legislation in accordance with the eight stated data protection principles outlined in the Act as follows:

1) Obtain and process information fairly.
   - COOL HARBOUR will obtain and process personal data fairly and in accordance with the fulfillment of its functions.

2) Keep data only for one or more specified, explicit and lawful purposes.
   - COOL HARBOUR will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

3) Use and disclose data only in ways compatible with these purposes.
   - COOL HARBOUR will only disclose personal data that is necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

4) Keep data safe and secure.
   - COOL HARBOUR will take appropriate security measures against unauthorized access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. COOL HARBOUR is aware that high standards of security are essential for all personal data.

5) Keep data accurate, complete and up-to-date.
   - COOL HARBOUR will have procedures that are adequate to ensure high levels of data accuracy.
   - COOL HARBOUR will examine the general requirement to keep personal data up-to-date.
   - COOL HARBOUR will put in place appropriate procedures to assist staff in keeping data up-to-date.

6) Ensure that data are adequate, relevant and not excessive.
   - Personal data held by COOL HARBOUR will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept.

7) Retain data for no longer than is necessary for the purpose or purposes for which they are kept.

8) Give a copy of his/her personal data to that individual, on request.
   - COOL HARBOUR has procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation. The operation of the Information Security Management System (ISMS) in compliance with ISO 27001 requirement is a key part of our commitment.

5. Privacy by Design

COOL HARBOUR had adopted the principle of privacy by design and will ensure that the organization and planning of all new or significantly changed system that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes.
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
- Assessment of the risks to individuals in processing the personal data.
- What controls are necessary to address the identified risks and demonstrate compliance with legislation.

6. Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.
Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

7. Definitions

The following definitions are taken from the Data Protection Acts 1998 and 2003. Full copies of the act are available at the Data Protection Commissioner web site and internally controlled as per our Legal and Other Requirements Procedure.

- Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

- Sensitive personal data means personal data as to:

  - The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject
  - Whether the data subject is a member of a trade-union
  - The physical or mental health or condition or sexual life of the data subject
  - The commission or alleged commission of any offence by the data subject, or
  - Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

- Processing means any operation or set of operation which is performed on personal data or on sets of personal data, whether or not automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or otherwise making available, alignment or combination, restriction erasure or destruction.

- Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data – where the purposes and means of such processing are determined by Union or Member State law, the controller or specific criteria for its nomination may be provided for Union or State law.

8. Procedures and Guidelines

This policy supports the provision of a structure to assist in COOL HARBOUR's compliance with the Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection. The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way COOL HARBOUR carries out its information processing activities. It is the company's policy to ensure to ensure that our compliance GDPR and other relevant legislation is always clear and demonstrable. The policy also supports COOL HARBOUR's compliance with guidance on maintaining confidentiality in relation to all records.

9. Breach Notification

It is COOL HARBOUR policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure.

10. Addressing Compliance to the GDPR

The following actions are undertaken to ensure that COOL HARBOUR complies at all times with the accountability principle of the GDPR:

- Clear and unambiguous legal basis for processing personal data.
- All staff to understand their responsibilities for following good data protection practice, when handling personal data.
- All staff trained in data protection.
- Consent rules followed.
- Personal data related procedures regularly reviewed.
- All new or changed systems and process to follow/adopt Privacy by Design principles.
- The following documentation of processing activities is recorded:
  - Organization name and relevant details.
  - Purposes of the personal data processing.
  - Categories of individuals and personal data processed.
  - Categories of personal data recipients.

- Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place.
- Personal data retention schedules.
- Relevant technical and organisational controls in place.

The above listed actions will be reviewed on a regular basis as per our Management Review procedure.

11. Obligations as a Cloud Service Provider

In addition to holding personal data on our own account, COOL HARBOUR, also stores and processes the personal data of our cloud customers. Our policy in this area is informed by ISO/IEC 27018- Code of practice for protection of personally identifiable information (**PII**) in public clouds acting as PH processors which, as well as recommending specific enhancements to ISO/IEC 27001 controls, also provides the following policy guidance:

- We must provide our customers with the facilities to meet their obligations under law in activities such as accessing, amending and erasing individuals' PII.
- We must only use the cloud customer's PII for their purposes, not our own.
- The customer must be informed if we are required by law to disclose any of their data, unless we are prohibited from doing so.
- Details of disclosures must be recorded.
- We must tell our customers if we use sub-contractors to process their PII.
- We must tell our customers if their PII is subject to unauthorized access.
- It must be clear in which country or countries the customer's PII is stored.

Additional recommendations stated in ISO/IEC 27018 are also included in the relevant policies and procedures within the ISMS

12. Roles/Responsibilities

COOL HARBOUR has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees of COOL HARBOUR who collect and/or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation. COOL HARBOUR will provide support, assistance, advice and training to all staff to ensure it is in a position to comply with the legislation.

COOL HARBOUR is registered as a Data Controller in compliance the Act and the following roles are included in the registration:

- Contact Person – Derek O' Herlihy
- Compliance Person – Denis Croombs
- Coordinator – Brian English

13. Review

This Policy will be reviewed regularly in light of any legislative or other relevant indicators.

14. Policy Approval

Derek O' Herlihy
CEO, COOL HARBOUR, Ltd.
02nd May 2019