Data Retention & Disposal

(a) Records need to be properly recorded, retained & disposed of to comply with GDPR and to enable us to meet our business needs, legal requirements, to evidence events or agreements in the event of allegations or disputes and to ensure that any records of historic value are preserved.

(b) The untimely destruction of records could affect:

- the conduct of our business;
- our ability to defend or instigate legal actions;
- our ability to comply with statutory obligations;
- our reputation.

(a) Conversely, the permanent retention of records is undesirable and disposal is necessary to free up storage space, reduce administrative burden and to ensure that we do not unlawfully retain records for longer than necessary (particularly those containing personal data).

(b) This policy supports the Organisation in demonstrating public accountability through the proper retention of records and by demonstrating that disposal decisions are taken with proper authority and in accordance with due process.

Purpose

(c) The purpose of this policy is to set out the length of time that our records should be retained and the processes for disposing of records at the end of the retention period.

Scope

(d) The policy covers the records listed in the schedule to the policy set out in our Employee Information Data Retention and Disposal Schedule ('the Schedule') irrespective of the media on which they are created or held including:

- paper;
- electronic files (including database, Word, Powerpoint presentations, spreadsheets, webpages and e-mails);
- photographs, scanned images, CD-ROMs and video tapes.

(e) The Schedule aims to include all types of records which we create or holds. They include:

- minutes of meetings;
- submissions from external parties;
- contracts and invoices;
- registers;
- legal advice;
- file notes;
- financial accounts;
- employee information;
- the Organisation's publications.

(f) Should you become aware of any records missing from the Schedule, please notify the person responsible for Information Technology (IT) so that they may be added at the next opportunity.

Application

(g) The policy applies equally to full time and part time employees on a substantive or fixed-term contract and to associated persons who work for us such as Board Members, agency staff, volunteers, contractors and others employed under a contract of service.

(h) The Chairperson of the Board of Trustees is responsible for ensuring that this policy is applied within New Quay Memorial Hall.

(i) The Chairperson of the Board of Trustees has lead responsibility for records management within New Quay Memorial Hall.

Minimum retention period

(j) A recommended minimum retention period is provided for each category of record in our **Employee Information Data Retention and Disposal Schedule ('the Schedule')**. The retention period applies to all records within that category. The recommended minimum retention period derives from either:

- business need as determined by the Board/Senior Management Team; or
- legislation.

Disposition

(k) The Chairperson of the Board of Trustees is responsible for ensuring that the Schedule is periodically reviewed (at least annually) to determine whether any retention periods applying to records have expired. Once the retention period has expired, the record must be reviewed and a 'disposition action' agreed upon.

(l) A 'disposition action' is either:

a) the destruction of the record; or
b) the retention of the record for a further period within the Organisation.

(m) Each of these options is described further below.

Making and Recording the Disposition Decision

(n) A review of the record should take place as soon as possible after the expiry of the retention period. It need not be a detailed or time-consuming exercise but there must be a considered appraisal of the contents of the record. The review should be conducted by the relevant Trustee (or their delegate) in consultation with relevant stakeholders for example:

- other senior Manager/the Trusteess;
- person responsible for IT;
- relevant external bodies;
- legal adviser.

(o) The disposition decision must be reached having regard to:

- on-going business and accountability needs (including audit);
- current applicable legislation (including GDPR);
- whether the record has any long-term historical or research value;
- best practice in the applicable professional field (for example human resources);
- costs associated with continued storage versus costs of destruction;
- the legal, political and reputational risks associated with keeping, destroying or losing control over the record.

(p) Decisions must not be made with the intent of denying access or destroying evidence.

(q) The agreed disposal decision must be recorded on a Record Disposal Form. The form will require the following information:

- Description of the record;
- The medium on which it is held e.g. CD;
- The directorate which created or held the record;
- The date of the creation of the record and the date of review;
- The disposal decision and the method of disposal;
- A summary of the reasons for the decision;
- The titles of the reviewers and officers consulted;
- The signature of the person authorising disposal.

Completed forms must be passed to the person responsible for IT for safekeeping.

Destruction

IMPORTANT!

(r) No destruction of a record should take place without assurance that:

- the record is no longer required by any part of the business;
- no work is outstanding by any part of the business;
- no litigation or investigation is current or pending which affects the record;
- there are no current or pending FOIA or GDPR access requests which affect the record.

Destruction of Paper Records

(s) Destruction should be carried out in a way that preserves the confidentiality of the record. Non-confidential records i.e. records that are clearly in the 'public domain' can be placed in ordinary rubbish bins or recycling bins. Confidential records should be placed in the grey confidential waste bins or shredded and placed in paper rubbish sacks for collection by an approved disposal firm. All copies including security copies, preservation copies and backup copies should be destroyed at the same time in the same manner.

Destruction of Electronic Records

(t) All electronic records will need to be either physically destroyed (and a record of destruction certified) or wiped to the current Government standard. Deletion of the files is not sufficient. Destruction will be overseen by the person responsible for IT.

Further Retention within the Organisation

(u) The record may be retained for a further period if it has on-going business value or if there is specific legislation which requires it to be held for a further period.