1. Strategic Overview

Background

The original Cornwall Heritage Trust IT platform was based on PCs and the Microsoft Windows operating system. After a few years the PC became so slow that the technology had to be replaced. At the same time, the number of staff and trustees needing to access online facilities at the office was increasing and there was also a need to be able to access presentations, files and emails out of the office.

A review of the office IT requirements took place and it was decided to change the technology platform to Apple Macs for the following reasons:

- Cornwall Heritage Trust does not have access to a dedicated IT department and Apple Macs are far less vulnerable to virus attack and ransomware.
- Although the initial cost of the technology is more expensive, the Apple Macs tend to retain their efficiency and response times for a greater length of time. Therefore the lifetime cost is generally less.
- There was a desire to bring more design work in house and Apple Macs are ideal for publishing purposes.

In addition, it was decided that all the technology should be capable of networking, should be compatible with Quickbooks.

As a result of the review, two iMacs were purchased and networked. A MacBook Pro was also purchased for use away from the office. iCloud was used for data storage. A further iMac has been purchased due to taking on additional staff.

It was agreed that an IT policy should be developed and maintained to reflect the increasing complexity of the office systems. This IT policy is additional to the following policies both of which can be found in the footer of the website

i) Privacy Policy
ii) Cookie Policy

The office now uses a CRM system called e-Tapestry which is also Cloud based. This database contains personal details of members and supporters and therefore it is particularly important that staff maintain strict security of the data and are aware of 'Acceptable Usage'.

2. Acceptable Usage

'Acceptable Usage' covers the security and use of all Cornwall Heritage Trust's information and IT equipment.

It also includes the use of databases, email, internet, intranet, voice and mobile IT equipment. This policy applies to all Cornwall Heritage Trust's employees, contractors, volunteers and trustees who use the office equipment or access the network or intranet (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Cornwall Heritage Trust's business activities and to all information handled by Cornwall Heritage Trust relating to other organisations with whom it deals.
It also covers all IT and information communications facilities operated by Cornwall Heritage Trust or on its behalf.

i) **Access Control – Individual's Responsibility**

Access to the Cornwall Heritage Trust IT systems is controlled by the use of User IDs and passwords.

All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Cornwall Heritage Trust's IT systems.

Individuals must not:

• Allow anyone else to use their user ID and password on any Cornwall Heritage Trust IT system.

• Leave their user accounts logged in at an unattended and unlocked computer.

• Use someone else's user ID and password to access Cornwall Heritage Trust's IT systems.

• Leave their password unprotected (for example writing it down).

• Perform any unauthorised changes to Cornwall Heritage Trust's IT systems or information.

• Attempt to access data that they are not authorised to use or access.

• Exceed the limits of their authorisation or specific business need to interrogate the system or data.

• Connect any non-Cornwall Heritage Trust authorised device to the Cornwall Heritage Trust network or IT systems.

• Store Cornwall Heritage Trust's data on any non-authorised Cornwall Heritage Trust equipment. This includes staff and Trustee's personal IT equipment.

• Give or transfer Cornwall Heritage Trust data or software to any person or organisation outside Cornwall Heritage Trust without the authority of the Chief Executive Officer.

The Chief Executive Officer must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

ii) **Internet and email - Conditions of Use**

Use of Cornwall Heritage Trust's internet and email is intended for business use.

Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Cornwall Heritage Trust in any way, not in breach of any term and condition of employment and does not place the individual or Cornwall Heritage Trust in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

• Use the internet or email for the purposes of harassment or abuse.

• Use profanity, obscenities, or derogatory remarks in communications.

• Access, download, send or receive any data (including images), which Cornwall Heritage Trust considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

• Use the internet or email to make personal gains or conduct a personal business.

• Use the internet or email to gamble.

• Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

• Place any information on the Internet that relates to Cornwall Heritage Trust, alter any information about it, or express any opinion about Cornwall Heritage Trust, unless they are specifically authorised to do this.

• Send unprotected sensitive or confidential information externally.

• Forward Cornwall Heritage Trust's mail to personal (non-Cornwall Heritage Trust) email accounts (for example a personal Hotmail account).

• Make official commitments through the internet or email on behalf of Cornwall Heritage Trust unless authorised to do so.

• Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.

• In any way infringe any copyright, database rights, trademarks or other intellectual property.

• Download any software from the internet without prior approval of the IT nominated member of staff.

• Connect Cornwall Heritage Trust devices to the internet using non-standard connections.

iii) **Clear Desk and Clear Screen Policy**

In order to reduce the risk of unauthorised access or loss of information, Cornwall Heritage Trust enforces a clear desk and screen policy as follows:

• Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

• Care must be taken to not leave confidential material on printers or photocopiers.

• All business-related printed matter must be disposed of using confidential waste bins or shredders.

iv) **Working Off-site**

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

• Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.

• Laptops must be carried as hand luggage when travelling.

• Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN.

v) **Mobile Storage Devices**

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.

vi) **Software**

Individuals must use only software that is authorised by Cornwall Heritage Trust.

Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Cornwall Heritage Trust computers must be approved and installed by the Cornwall Heritage Trust IT nominated individual.

Individuals must not store personal files such as music, video, photographs or games on Cornwall Heritage Trust IT equipment.

vii) **Viruses**

The IT department has implemented centralised, automated virus detection and virus software updates within the Cornwall Heritage Trust. All computers have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

• Remove or disable anti-virus software.

• Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Cornwall Heritage Trust anti-virus software and procedures.

viii) **Telephony (Voice) Equipment Conditions of Use**

Use of Cornwall Heritage Trust voice equipment is intended for business use. Individuals must not use Cornwall Heritage Trust's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

• Use Cornwall Heritage Trust's voice for conducting private business.

• Make hoax or threatening calls to internal or external destinations.

• Accept reverse charge calls from domestic or International operators, unless it is for business use.

ix) **Actions upon Termination of Contract / Trusteeship**

All Cornwall Heritage Trust equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Cornwall Heritage Trust at termination of contract (including Trustees).

All Cornwall Heritage Trust data or intellectual property developed or gained during the period of employment/Trusteeship remains the property of Cornwall Heritage Trust and must not be retained beyond termination or reused for any other purpose.

x) **Monitoring and Filtering**

All data that is created and stored on Cornwall Heritage Trust computers is the property of Cornwall Heritage Trust and there is no official provision for an individual's data privacy, however wherever possible Cornwall Heritage Trust will avoid opening personal emails.

Cornwall Heritage Trust has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

3. Enforcement

i) Training

Any individual who has access to the network or the computers and mobile devices at Cornwall Heritage Trust should be made aware of the IT Policy and the Privacy Policy. They should also sign a form to say they have read and understood these policies.

This provides documented proof that an individual has not only been made aware of the policies, but also that they have actively agreed to adhere to them. The individual should be provided with a copy of the signed form as well.

A record should be kept of any violations of policies.

ii) Quality Assurance

A nominated IT individual and the Chief Executive Officer should review the IT and Privacy Policies once every 6 months and make any necessary amendments. There should be strict revision control in recording amendments and good communication of revisions throughout the organisation.

4. Current Procedures

i) Backups and storage

'Time Machine' is used to back up the server at regular intervals and the Chief Executive Officer manually backs up the files to an external hard drive, the server automatically backs up to secure cloud-based storage.

ii) Changes to Passwords

All staff have their own passwords to the machines and also to access the server, emails and various online systems such as eTapestry and Quickbooks. These should be changed if they suspect a breach.

iii) Access to Office

All staff have a key but the office is always locked when empty.