ICT Policy

1. Introduction

1.1 This policy outlines the principles and standards we require those using our computer devices, systems, technology, internet, e-mail and other communications systems (hereafter referred to as 'technology') to observe and comply with. It also explains when we will monitor the use of technology and the action we will take if the terms of this policy are breached.

1.2 This policy applies to the use of The St Andrews Preservation Trust Ltd's, hereon in referred to as "The Charity", technology on our premises and any other place where we conduct our business/operations/services, and also when using our technology from any other place including, for some people (where permitted), your home. It applies to all our employees, agency workers, secondees, placements, volunteers, workers, consultants and other contractors who have access to our technology.

1.3 This policy applies to personal use of our technology. It also applies to the use of personal computers, smartphones or other technology devices including storage devices on our premises and/or connecting such equipment to our technology. This policy also applies to the use of any technology not belonging to, or operated by the, Charity but used by you during working hours.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

1.5 The Administrator is responsible for the monitoring and implementation of this policy. Any questions about the content or application of this policy or other comments should be referred to The Administrator.

1.6 It is important that you read and understand this policy. We appreciate that people have differing levels of technical knowledge, so if you are unsure about any of the terminology used in this policy you should speak to the Administrator.

2. Use of the Company's technology

2.1 You may use our technology only to the extent that you are authorised to do so. You should not use our technology for any purpose that is not connected to our business unless you have express permission to do so or you are making personal use of the system as permitted by this policy (see section 9). Use of our technology for commercial purposes other than our business is strictly prohibited.

2.2 If you have access to our network you must adhere to strict access controls, to reduce the risk of virus infections, hacking and other unauthorised access attempts:

2.2.1 only authorised technology is allowed to connect to our network from any location;

2.2.2 remote access (via broadband, dial-up, mobile network etc.) is also restricted to authorised technology and access must only be via secure means, e.g. a Virtual Private Network (VPN) connection or similar;

2.2.3 the only access allowed to unauthorised technology, e.g. internet café terminals, is subject to such technical or other measures as explicitly stated by the Administrator.

2.3 We license software from a number of sources. We do not own that software and must comply with any restrictions or limitations on use, in accordance with licence agreements. You must adhere to the provisions of any software licence agreements to which we are party.

2.4 You must not use any software for any purpose outside our business without express permission of the Administrator or as otherwise permitted by the terms of this policy and you must not copy, download or install any software without first obtaining permission from the Administrator.

3. Confidentiality

3.1 You should never assume that internal or external messages are necessarily private and confidential, even if marked as such. E-mail and the internet are not secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an e-mail, which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by e-mail unless unavoidable and if so, should be clearly marked in the message header as highly confidential, and should be encrypted or, at an absolute minimum, password protected where this is possible. The confidentiality of internal communications can only be ensured if they are personally by hand or included in a password-protected or encrypted online document.

3.2 You should refer to the Confidentiality Policy for details of the types of information that we regard as confidential and which should be treated with particular care.

4. General rules regarding communications and e-mail

4.1 All communications, including e-mail, should reflect the highest professional standards at all times. In particular, you must:

4.1.1 keep messages brief and to the point;

4.1.2 ensure the spelling and grammar are carefully checked before sending;

4.1.3 ensure that all e-mails sent from us include. "This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail in error please notify our Administrator by telephoning 01334477152".

4.1.4 ensure that an appropriate heading is inserted in the subject field; and

4.1.5 double check the recipient(s) before pressing the send button-not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about us or a client/customer/member/service user and/or a breach of our data protection obligations.

4.2 You must not send messages from another person's e-mail address (unless authorised in the proper performance of your duties) or under an assumed name.

4.3 You must not send offensive, demeaning, disruptive or defamatory messages or images by any method. Or any sexist or racist material or any material which could be offensive on the grounds of a person's disability, age, sexual orientation, gender or religion or belief.

4.4 You must not place on any systems or send any message or image which could be regarded as personal, potentially offensive or frivolous.

4.5 If you receive any communication containing material that is offensive or inappropriate to the workplace environment, you must delete it immediately. Under no circumstances should such communication be forwarded either internally or externally, other than internally to the Administrator in order to report a breach of this policy.

4.6 You should not transmit anything in an e-mail or other communication that you would not be comfortable writing (or someone else reading) in a letter. E-mails leave a retrievable record and, even

when deleted, can remain on computers and back-up systems. E-mails can be recovered and used as evidence in court proceedings and/or reviewed by regulators. Electronic messages are admissible as evidence in legal proceedings and have been used successfully in defamation and discrimination cases.

4.7 You must not create congestion on our systems by sending trivial messages or by unnecessary copying or forwarding of messages to recipients who do not need to receive them, or by sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.

4.8 You must use a Trust e-mail address for sending and receiving work-related e-mails and must not use your own personal e-mail accounts to send or receive e-mails for the purposes of our business. You must not send (inside or outside work) any message in our name unless it is for an authorised, work-related purpose.

4.9 You must not send unsolicited commercial e-mails to persons with whom you do not have a prior relationship without the express permission of the Administrator.

4.10 Communications must not use our logos and other branding material without the approval of the Communications Committee.

4.11 Communications must not provide references or recommendations for any third party, unless expressly authorised by Communications Committee.

4.12 E-mails will be stored on office 365 for 6 months after which they will be permanently deleted. Any customer/client/service-user/member-related e-mails should be saved and/or printed or filed within the Trust's filing system.

5. Passwords

5.1 You are personally responsible for the security of all equipment allocated to or used by you. You must not allow equipment allocated to you to be used by any other person, other than in accordance with this policy.

5.2 Any IT equipment allocated to you must be secured appropriately. Depending on the device, such security might be a password, PIN, fingerprint recognition, facial recognition, or gesture recognition. Any security method other than those involving facial, fingerprint or other biometric recognition should be changed on a regular basis and must be kept confidential.

5.3 You must not use another person's username and/or password to access our systems, nor allow any other person to use your password(s). If it is anticipated that someone may need access to your confidential files in your absence, you should arrange for the files to be copied to a network location that is properly secure where the other person can access them, or give the person temporary access to the relevant personal folders. Nobody in the Charity other than the Administrator or Chairman shall ever ask you for your password, and any request contrary to this should be refused and reported to the Administrator.

5.4 Occasionally, a third party may need access to your machine (e.g. to provide IT support). Such access must be approved by Quest IT. In such instances, you must close all browsers, files or programs that show confidential or personal data before permitting access. You must not permit the third party to access the systems unsupervised, including when this is by remote access, and you should actively monitor their activity.

5.5 You must log out of the system or lock your computer when leaving your desk for any period of

time. You must log out and shut down your computer at the end of the working day. You must ensure that any physical copies of documents/data that are caused to be produced (i.e. printed) are uplifted timeously and are not left unattended for any period of time.

6. Contact lists

6.1 Lists of contacts compiled by you during the course of your time with the Charity and stored on our e-mail system, database(s) or other systems (irrespective of how they are accessed) belong to us. Such lists, or parts of the lists, may not be copied or removed by you for use outside of your role with the Charity or after your role ends.

7. Systems and data security

7.1 Be vigilant when using our e-mail system. Computer viruses are often sent by e-mail and can cause significant damage to our information systems. Be particularly cautious in relation to unsolicited e-mail from unknown sources.

7.2 If you suspect that an e-mail may contain a virus, you should not reply to it, open any attachments to it or click on any links in it and you must contact Quest IT immediately for advice.

7.3 You must not download or install software from external sources without prior authorisation from the Administrator. Files and other software should be downloaded only from trusted sources, and should be subjected to a virus scan before opening/running.

7.4 Personal computer, mobile phone, tablet computer, USB storage device or other device are permitted to be connected to our systems or network with prior permission from the Administrator. Any permitted equipment must have up-to-date anti-virus software installed on it and we may inspect such equipment in order to verify this. You must not connect any such device to any of our technology if you suspect there may be a virus or other malicious software on it. All personal devices must logged as using our network.

7.5 You must not run any '.exe' files, particularly those received via e-mail, unless authorised to do so in advance by the Quest IT. Unauthorised files should be deleted immediately upon receipt without being opened.

7.6 You must not access or attempt to access any password-protected or restricted parts of our systems for which you are not an authorised user.

7.7 You must inform Quest IT immediately if you suspect your computer may have a virus and must not use the computer again until informed it is safe to do so. You must also disconnect the machine from any organisation networks immediately and turn the machine off.

7.8 All laptop, tablet, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

8. The internet

8.1 Access to the internet during working time (or the time during which you should be performing your role for the Charity) is primarily for matters relating to your role/work duties and employment. Reasonable, limited personal use of the internet is permitted in accordance with paragraph 9.

8.2 Any unauthorised use of the internet is strictly prohibited. Unauthorised use includes (but is not limited to):

8.2.1 creating, viewing, accessing any webpage or posting, transmitting or downloading any image, file or other information unrelated to your employment and, in particular, which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us or to our clients/customers;
8.2.2 engaging in computer hacking and/or other related activities; and
8.2.3 attempting to disable or compromise security of information contained on our systems or those of a third party.

8.3 You are reminded that such activity may also constitute a criminal offence under the Computer Misuse Act 1990, or other relevant legislation. Where a criminal offence has been committed, we may (and in some cases, must) report these offences to the relevant authorities.

8.4 Postings/messages placed on the internet may display our address or in some other way be traced to the Charity. For this reason, you should make certain before posting information that the information reflects our standards and policies. Under no circumstances should information of a confidential or sensitive nature be placed on the internet. You must not use our name in any internet posting (inside or outside work) unless it is for a work-related purpose and you have the authority to do so.

8.5 Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the internet may be done only by express permission from the copyright holder. You must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer program.

8.6 You must not commit us to any form of contract through the internet without the express permission of your line manager.

8.7 Subscriptions to news groups, mailing lists and social networking websites are permitted only when the subscription is for a work-related purpose. Any other subscriptions are prohibited. You are reminded that we have a separate Social Media Policy, which must be adhered to at all times.

8.8 We may block or restrict access to any website, application or network at our discretion.

9. Personal use of our systems
9.1 We do not permit any personal use of our systems to send personal e-mail, browse the internet or make personal telephone calls.

10. Use of personal devices
10.1 The organisation recognises and welcomes the benefits offered to users in using their own devices for work purposes. However, where work is done on personal devices, this can significantly increase the risk of data being compromised through the loss, theft, use or exploitation of weaknesses in personal devices. Users must be especially mindful of, and take precautions against, these additional risks.

10.2 The precautions that a user should reasonably take may depend on whether their use of personal devices is high-risk or not. High-risk users must take all precautions listed in column 1 and 2; all other users are strongly advised to follow at the bare minimum the precautions in column 2. If you are not sure whether you are a high-risk user, you must assume that you are high-risk. This category will typically include anyone processing special categories of personal data or sensitive data, or high volumes of confidential data, and will include most managers, Trustees, Finance officers, HR officers and the like.

Column 1 - minimum requirements	Column 2 - good practice (and essential for high risk users)
Set up a strong password, pin or commensurate security system on the device, and keep this absolutely secret.	Regularly delete copies of documents from your device when no longer required, regardless of whether they contain sensitive data or not. When you replace the device, or are no longer associated with the organisation, delete everything related to the organisation.
Lock your device when not in use and ensure that it is set to lock automatically when inactive for more than a couple of minutes.	Encrypt all data where possible.
Do not leave your device unattended, and ensure that it is stored in a secure, private place.	Report any data or system breaches.
Ensure that all relevant software (especially anti-virus) is up-to-date with the latest security patches. Also ensure that there is a strong firewall in place, and that you do not insert any USB, CD or other media of unknown or questionable provenance. Only install apps and software from reputable providers (e.g Windows Store, Apple Store, Play Store).	Ensure that your device is configured with security in mind, using the latest technology available to you.
Ensure that documents are backed up as often as possible on the organisation's main server/Sharepoint site/storage location.	Where using mobile devices, ensure that you have a remote wipe option that can be used if required.
If the device is shared with others (e.g. family member) ensure that they have no access to sensitive organisation data (e.g. e-mail accounts) and consider using multiple profiles on the device to segregate users.	Do not connect to open and unsecured Wifi networks, and disable services such as Bluetooth or Wifi when not in use.
Before using a second-hand device, reset it fully to factory settings to ensure that no malware is present on the system.	

10.2 Where a user fails in their obligations under this section, they may be guilty of misconduct or gross misconduct under our disciplinary policy.

11. Telephone Calls

11.1 The Charity does not monitor or record external telephone usage.

11.2 The telephone system is not a personal telephone system and you are not generally permitted to use our telephone system except for legitimate business purposes or for limited personal use where this is infrequent, inexpensive and the purposes do not constitute a misuse of the system (as defined below). You may be able to make expensive calls (e.g. long distance, international etc.) under certain circumstances subject to obtaining prior authorisation. The Charity will charge you for costs incurred in such circumstances.

11.3 Charity telephone numbers (any number operated by the Charity, including Direct Dial Inward (DDI) numbers) may not be used for personal matters except where this is infrequent and does not constitute a misuse of the system as defined below.

11.4 Misuse of the telephone system may result in disciplinary action up to, and including, dismissal. Examples of misuse include, but are not limited to, the following:

11.4.1 Calling premium lines;

11.4.2 Calls of a sexual nature;

11.4.3 Calls of an intimidating, threatening or harassing nature;

11.4.4 Calls involving profanities, obscene or offensive language;

11.4.5 Discussions relating to persons or matters likely to bring harm or ill repute to the Charity, its directors, employees, volunteers or clients either directly or indirectly.

12. Monitoring

12.1 Our systems enable us to monitor e-mail, voice-mail, internet and other communications. Your use (including personal use) of our systems may be monitored by automated software or otherwise, for business reasons, in order to carry out our obligations as an employer, in order to monitor compliance with the terms of this policy or in rare cases to comply with a regulatory or legal investigation or requirement.

12.2 We do not as a matter of policy routinely monitor your use of the internet or the content of e-mail messages sent or received. However, we have a right to protect the security of our systems and reputation of the Charity and will occasionally check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon us. To achieve these objectives, we carry out random spot checks on the system which may include accessing your e-mail messages or checking on specific internet sites searched for and/or accessed by you.

13. Prohibited use and breach of this policy

13.1 We consider this policy to be extremely important. Any breach of the policy will be dealt with under our Code of Conduct and Dismissal and Disciplinary Procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, we may withdraw your internet and/or e-mail access.

13.2 Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

13.2.1 unauthorised use of the internet as outlined in paragraph 8.2 above;

13.2.2 creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;

13.2.3 creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in our [Equality OR Equal Opportunities] Policy and our Harassment and Bullying Policy;

13.2.4 accessing, transmitting or downloading any confidential information about the Charity and/or any of our staff/volunteers/secondees/placements/consultants and/or clients/service users/members/customers, except where authorised in the proper performance of your duties;

13.2.5 accessing, transmitting or downloading unauthorised software; and

13.2.6 viewing, accessing, transmitting or downloading any material in breach of copyright.