Acts Trust Bring Your Own Device Policy

1. Purpose of this Policy:

1.1. This policy defines the relationship and responsibilities between the Employee/Volunteer and Acts Trust when the Employee/Volunteer uses their own device (laptop, phone, tablet etc) to carry out duties on behalf of the Trust.

1.2. Acts Trust will provide all devices deemed necessary for all Employees/Volunteers for the purpose of carrying out work duties. However, Acts Trust grants Employees/Volunteers the privilege of using personal smartphones, tablets and laptops of their choosing at work if preferred for their convenience. Acts Trust reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

1.3. This policy is intended to protect the security and integrity of Acts Trust's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

1.4. Acts Employees/Volunteers must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the network/ used for work purposes in a work environment/setting.

2. Acceptable Use

2.1. The Trust defines acceptable business use as activities that directly or indirectly support the work of Acts Trust.

2.2. The Trust defines acceptable personal use on Trust time as reasonable and limited personal communication or recreation, such as reading or game playing.

2.3. Devices may not be used at any time to:

- Store or transmit illicit content[1]
- Harass others

[1] Illicit content is defined as material that is considered illegal by the UK government, including pornography of any nature and video content content obtained without a copyright license (e.g Peer to peer video downloads)

- Engage in outside business activities during work hours

2.4. Employees/Volunteers may use their mobile device to access the following Trust-owned resources:

- email
- calendars
- contacts
- documents

2.5. Acts Trust has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

3. Devices and Support

3.1. All makes and models of smartphone, tablet or laptop are permitted

3.2. IT support will be provided for connectivity issues with the local network

3.3. All devices which are being used for Trust purposes must be presented for an annual PAT test (the cost of which will be provided if the device is to be your main work device).

4. Reimbursement

4.1. The Trust will not reimburse the employee for any percentage of the cost of the device

4.2. The Trust will cover the cost of the entire phone/data plan if the phone is to be used solely for work activity

4.3. The Trust will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

5. Security

5.1. In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the Trust network.

5.2. The Trust's strong password policy is: Passwords must be at least six characters and a combination of letters, numbers and symbols.

5.3. The device must lock itself with a password or PIN if it's idle for longer than five minutes.

5.4. Smartphones, tablets and laptops belonging to Employees/Volunteers that are for personal use only are/are not allowed to connect to the network without pre-approved consent from line manager.

5.5. No work data must be kept locally on a device hard drive without pre-approved consent from line manager. Data must only be accessed remotely (e.g: via cloud based drives)

5.6. If the employee's contract/ volunteer's agreement is terminated or ended, it is their responsibility to ensure no work data is left on the device, and access to any work networks including wifi must be removed.

5.7. The Trust reserve the right, upon termination of employment, to verify that all content has been transferred off an employee's device prior to their final day of employment.

6. Risks/Liabilities/Disclaimers

6.1. It is the employee/volunteer's responsibility to take precautions to protect personal data on devices, such as backing up personal email, contacts, pictures and files etc.

6.2. The Trust reserves the right to disconnect devices or disable services without notification.

6.3. Lost or stolen devices that Acts Trust pay the data plan for must be reported to the Trust within 24 hours. Employees/Volunteers are responsible for notifying the mobile carrier immediately upon loss of a device.

6.4. The employee/volunteer is expected to use his or her devices in an ethical manner at all times and adhere to the Trust's acceptable use policy as outlined above.

6.5. The employee/volunteer is personally liable for all costs associated with his or her device.

6.6. The employee/volunteer assumes full liability for risks including, but not limited to, the partial or complete loss of Trust and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

6.7. Acts Trust reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Signed agreement:

_____ (Employee/ Volunteer)

_____ (Line Manager)

_____ (Date)