Teddington & Hampton Wick Voluntary Care Group - Remote Working Policy

1 **Scope and definitions**

1.1 This policy applies to all staff who use or access TVCG information remotely either occasionally or as part of their contract. It applies to information in all formats, including manual records and electronic data.

1.2 ‘Remote working’ means working out of the normal office environment.

1.3 ‘Staff’ includes anyone working on behalf of the TVCG or given access to TVCG data, e.g. volunteers

2 **Purpose**

2.1 To ensure that staff are aware of their individual responsibilities around information security when working remotely.

2.2 To ensure staff work in accordance with the TVCG information privacy policy.

2.3 To provide policy and guidance for staff on secure remote working and so minimise the risk of unauthorised access to, and loss of, data.

3 **Background and risks**

3.1 Remote working presents both significant risks and benefits for the TVCG.

3.2 Staff may have remote access to information held on the secure office computer but without the physical protections available and the network protections provided by firewalls and access controls there are much greater risks of unauthorised access to, and loss or destruction of, data. There are also greater risks posed by information ‘in transit’.

3.3 The risks posed by remote working with TVCG information can lead to loss of trust or damage to the TVCG’s relationship with its clients and volunteers

4 **Roles and responsibilities**

4.1 Any member of staff working remotely is responsible for ensuring that they work securely and protect both information and TVCG’s equipment from loss, damage or unauthorised access.

4.2 The committee are responsible for supporting their staff’s adherence with this policy.

4.3 Failure to comply with TVCG’s privacy and data protection policies may result in disciplinary action.

5 **Policy statement**

Staff working remotely must ensure that they work in a secure and authorised manner as set out in the Key principles below.

6 **Key principles**

The policy statement in 5 above is underpinned by the following Key principles. All staff must comply with these principles when working remotely.

- Do not use IT equipment where it can be overlooked by unauthorised persons and do not leave it unattended in public places.
- Use automatic lock outs when IT equipment is left unattended.
- Ensure that the master copy of the record, whether paper or electronic, is not removed from TVCG premises.
- Where possible, IT equipment must be encrypted
- You should not work remotely if there is a risk to your health or safety, for example, during building work at home or in unsanitary conditions, or if there is not a satisfactory work space for you to use. It is the responsibility of the member of staff to ensure that the working environment and space is suitable for remote working.
- Before working remotely, you must have read and completed the TVCG's volunteer agreement form and have read the privacy and data protection policies.
- Do not use internet cafes, when accessing TVCG systems and data.
- Access to certain systems and services by those working remotely may be deliberately restricted or may require additional authentication methods. Any attempt to bypass these restrictions may lead to disciplinary action.
- Staff should be authorised to remotely access TVCG information or systems by the Data Controller or committee

Appendix 1 - before the remote working begins.

When the TVCG provides equipment to staff, e.g. encrypted memory storage it will supply devices which are appropriately configured to ensure that they are as effectively managed as devices in the secure office environment.

Staff who have been provided with TVCG owned IT equipment to work remotely must:

- only use this equipment for legitimate TVCG purposes
- not modify it unless authorised by the data protection officer or committee
- return the equipment at the end of the remote working arrangement or prior to the recipient leaving the TVCG and not allow non-staff members (including family and friends) to use the equipment.
- not use an unsecured network

Users who process TVCG-held information on privately-owned equipment are responsible for the security of the device

Staff working remotely must ensure that information is retrievable. The access to information regimes – freedom of information and data Protection - gives the public rights of access to information held by the TVCG, and this covers information held remotely. In the event of a request for information staff must retrieve *all* relevant requested information, whether held remotely or in the TVCG office and within a reasonable time so that the TVCG can meet the relevant statutory deadlines for responding.

Staff working remotely must adhere to the TVCG privacy policy records and data protection guidelines, and in particular ensure that information held remotely is managed and securely deleted or destroyed once it is no longer necessary to process it remotely.

All staff, volunteers and others who work on behalf of the TVCG must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any TVCG owned IT equipment or data immediately to the data protection officer and committee in order that appropriate steps may be taken quickly to protect TVCG's data. Failure to do so immediately may seriously compromise TVCG's security and, for staff, may lead to investigation and potentially disciplinary procedures.