IT ACCEPTABLE USE POLICY

1.0 Purpose

TRGL seeks to facilitate the proper use of Information Technology (IT) for the purposes of supporting the activities of TRGL, its members and volunteers and other users of its facilities.

It is the responsibility of all Users of TRGL's IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

This Acceptable Use Policy is intended to provide a framework governing the use of all IT resources which TRGL operates. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

2.0 Scope

This policy applies to all Users including staff, Friends, Members, volunteers, visitors, contractors, partners, and others. Use of the IT facilities provided by TRGL, is bound by the provisions of its policies in addition to this Acceptable Use Policy. It includes the use of TRGL's IT facilities accessed via resources not owned by TRGL, such as personal equipment.

The IT facilities include hardware, software, data, storage, network access, telephony, printing, social media accounts, email accounts, back office systems and services and service provided by third parties including online, Cloud and hosted services.

3.0 Definitions of Unacceptable Use

TRGL's IT facilities include all computing, telecommunication, and networking facilities provided by TRGL, with particular reference to all computing devices, either personal or company owned, connected to systems and services supplied on-premises or remotely. They also include social media and email accounts operated by or on behalf of TRGL.

The conduct of all Users when using TRGL's IT facilities should always be in line with TRGL's values and acceptable conduct policy, including the use of online and social networking platforms.

Unacceptable use includes:

3.1. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

3.2. Creation or transmission of material which is subsequently used to facilitate harassment, bullying and/or victimisation of any party or which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation.

3.3. Creation or transmission of material with the intent to defraud or which is likely to deceive a third party or which advocates or promotes any unlawful act.

3.4. Creation or transmission of unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.

3.5. Creating unsolicited or bulk email (spam) or using mailing lists other than for legitimate purposes related TRGL's activities.

3.6. Using material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.

3.7. Creating, using or transmitting material that brings TRGL into disrepute.

3.8. Deliberately making unauthorised access to IT facilities or services or attempting to circumvent TRGL's security systems.

3.9. Any activity having, with reasonable likelihood, any of the following characteristics:

- Wasting staff effort or time unnecessarily on IT management.
    - Corrupting or destroying other users' data.
    - Violating the privacy of other users.
    - Disrupting the work of other users.
- Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
- Other misuse of network resources, such as the introduction of computer viruses, malware, or other harmful software.
- Introduce data-interception, password-detecting or similar software or devices to TRGL's equipment.

4.0 Monitoring

4.1. TRGL may monitor the use of its IT facilities for:

- The effective and efficient planning and operation of the IT facilities;
- Investigation, detection and prevention of infringement of the law, this policy or other TRGL policies;
- Investigation of alleged misconduct by users;

4.2. TRGL will comply with lawful requests for information from government and law enforcement agencies.

4.3. Users must not attempt to monitor the use of TRGL IT facilities without explicit authority to do so.

4.4. Access to workspaces, email, and/or individual IT usage information will not be given to another user unless authorised by the Board of Trustees

Consequences of Breach

In the event of any failure to comply with the conditions of this Acceptable Use Policy by a User, TRGL may in its sole discretion:

- Restrict or terminate a User's right to use any TRGL IT facilities.

- Withdraw or remove any material uploaded by that User in contravention of this Policy.
- Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.
- A breach of this policy may lead to disciplinary action which may ultimately lead to dismissal (in the case of members of staff), termination of Membership or membership of the Friends, or termination of contract.

Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the Board of Trustees.

Other notes

The use of TRGL IT systems and resources are subject to the following statutes and regulations:

- The Copyright, Designs and Patents Act 1988
- Computer, Copyright Software Amendment Act 1985
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- General Data Protection Regulation (GDPR) (EU) 2016/679
- The Electronic Communications Act 2000
- The Freedom of Information Act 2002
- The Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Criminal Justice and Public Order Act 1994

Copies of these documents are available online at http://www.opsi.gov.uk/

Document Control

Approval: 25th September 2021

By: Board of Trustees of Tavistock Repertory Guarantors Limited

Next review: September 2022