Data Security Policy June 2021

In order to comply with minimum standards of good practice, with the requirements of the District's cyber insurance carrier, and to protect our District Rotarians, the following initial data security policy is hereby adopted pertaining to District 5010 electronic media and communications:

1. This policy pertains to all persons with administrative-level access and privileges to any software and/or electronic platforms and social media used in connection with any District business.

2. This policy pertains to all electronic records, online platforms, and communications and other like and similar activities that involve or affect District 5010, including without limitation all youth activities, including ClubRunner, Wessex, YEAH, web site, Facebook, Google Suite, and like and similar software applications.

2. To the maximum extent practicable, the number of persons with administrative level privileges regarding any online platforms, databases, social media, web sites, communications shall be kept to the minimum necessary for the effective operation of the District and all its activities including Youth Exchange, RYLA, and social media. The listing of persons with current administrative level privileges shall be periodically reviewed to ensure compliance.

3. The District Administrative Consultant shall retain a current list of all persons with access and administrative privileges that are different and/or greater than those of Rotarians generally.

4. The District shall be a top level administrator on all such platforms and with the ability to appropriately limit access and administrative privileges by others.

5. All billings for every electronic platform, service, and application used by the District and its various activities in any way shall be billed directly to the District and paid by District.

6. The District shall be the domain name owner regarding all such online activities.

7. The District administrative officer(s) shall retain a listing of all such platforms along with current top-level administrative log-in credentials.

8. No person shall use any insecure software or online site on any computer or other device used for administrative level District electronic business. District-related business by those with administrative-level access shall be confined to a single device protected by security software provided at District expense.

9. The District shall determine and designate appropriate security software suites from time to time and shall provide protection at the District's expense to those devices used in connection with District business. District shall assist Rotarians with installation and initial use of such software. Such software will include a VPN (virtual private network) and should always be loaded at startup.

10. Unless authorized by a person, personal information such as Emails and telephone numbers shall not be posted in any publicly-accessible portion of the District web site, social media site, etc. but rather shall be posted inside the “login protection” area.

11. Persons to whom this policy pertains shall ensure that they are running both the basic security suite software and the VPN software.

12. The District will periodically provide software training to help you avoid falling into common malware traps. Please participate.

13. Admin-level users should review the accompanying data security “basics” information and conform to it.