

## APPENDIX G

### District Technology Guidelines and Procedures for Represented Certificated Staff

All access to the Internet is routed through a “technology protection measure” designed to filter out material that is in violation of the District’s Internet policies. This filter will block most objectionable material. Users should be aware that some objectionable material may be missed by the filter and users, upon discovering the presence of such material, shall report offending sites to the Technology and Information Services Branch Help Desk at extension 8411. Review processes are in place to block sites with objectionable material and to request the removal of blocks to sites that users believe contain material that has educational benefit. Finally, an adult filter is available if the user submits a request and receives approval from the appropriate Assistant Superintendent and the Executive Director of Information Services.

Represented certificated employees are responsible for following generally accepted social standards for use of a publicly owned and operated communication tool which includes various technology systems such as the Internet. Represented certificated staff will maintain high standards of ethical conduct while using all District technology systems. Examples of unethical, unacceptable use of District technology equipment include the following:

- Sending, displaying, or accessing pornographic, abusive, obscene, or other objectionable language, graphics, or other media
- Unauthorized disclosure, use, and dissemination of personal information about students or employees
- “Hacking” or otherwise engaging in unlawful computer or technology-oriented activities
- Using obscene language
- Harassing, insulting, or attacking others
- Intentionally damaging computers, computer systems, data, files, information or computer networks
- Violating copyright laws
- Using or distributing another’s password
- Trespassing in another’s digital folders, or files
- Intentionally wasting limited resources
- Employing the network for outside business or commercial purposes
- Sending or requesting of unethical, illegal, immoral, inappropriate, or unacceptable information of any type
- Engaging in activities that cause disruption to District technology systems
- Attempting to bypass District technology security measures
- Reposting or forwarding without the permission of the sender a message sent to you privately which is of a confidential nature or one clearly designed to be read by a limited number of selected recipients
- Posting chain letters or engaging in “spamming” – i.e., sending an annoying or otherwise unnecessary message to a large number of people

1 District technology is provided for represented certificated staff to conduct research, to  
2 communicate with others on academic topics, and to engage in legitimate District business.  
3 Individual users of the District technology are responsible for their behavior and  
4 communications on those networks. Users shall comply with District standards and will abide  
5 by the policies specified herein. Violations of the District policy described may result in access  
6 privileges being suspended or revoked, as well as other disciplinary action as warranted. Any  
7 commercial, political, or unauthorized use of District technology systems or services, in any  
8 form, is forbidden. All copyright laws must be observed.  
9

10 Members of the certificated teachers bargaining unit may engage in teacher association  
11 business on the District computer networks. Such teacher association business shall be  
12 conducted during non-duty hours which are defined in Article IV, Section C of this Agreement.  
13 Association use of District e-mails shall be limited to the following: authorized Association  
14 representatives may use District e-mails to provide notice of meetings, agendas for meetings,  
15 minutes of meetings, confirmation of a meeting with a District representative, or a limited  
16 distribution communique` between an authorized Chapter officer and a District representative;  
17 the Association will not use e-mail to denigrate the District or its personnel and will observe  
18 the prohibitions of Education Code, Section 7054.  
19

20 The Long Beach Unified School District respects the privacy of all certificated teacher users.  
21 System administrators and their staff may not log on to a user's account or view a user's files  
22 without explicit permission from the user. Exceptions arise when the user's account is  
23 suspected either of disrupting or endangering the security or integrity of any District  
24 technology system or service or of violations of applicable school district policies, federal or  
25 state law. Even then, the system administrator must normally obtain prior approval of the  
26 Executive Director of Information Services or the Deputy Superintendent of Education  
27 Services unless grave danger to the continued operation of the District's technology systems  
28 requires emergency action.  
29

30 This does not preclude Technology and Information Services staff from maintaining and  
31 monitoring system logs of user activity which access District technology systems. Moreover,  
32 automated searches for activities that endanger system security or integrity are preformed  
33 regularly to protect all users. Technology and Information Services administrators may take  
34 appropriate action in response to detection of such activity (typically removal of infected files  
35 and possibly suspension of the user's accounts until the matter can be resolved).  
36

37 Use of District technology systems may be revoked at any time for inappropriate use. The  
38 Technology and Information Services Branch, in collaboration with school administration, will  
39 be the sole determiners of what constitutes inappropriate behavior according to local, state, and  
40 federal law. The violation of any item contained in this policy may result in the loss of access  
41 and/or to District technology systems other disciplinary action, as well as possible punitive  
42 action as provided for by local, state, and federal law.  
43

44 The security of any information system is a high priority, especially any system that has many  
45 users and/or Internet access. Represented certificated staff members shall not let others use  
46 his or her account or password as he or she has a reasonable responsibility for all actions related

1 to his or her account. Certificated staff must notify school administrators immediately if their  
2 password is lost or stolen or if they think someone has access to their account. Represented  
3 certificated employees are to use only the network directories and resources that have been  
4 assigned for their use. Unauthorized access to any other level of the system, or other system  
5 resources, is strictly prohibited. Users will make no attempt to bypass the District anti-virus  
6 software, firewall, filtering and safeguards. When finished with a computer represented  
7 certificated employees are expected to logout where appropriate.  
8

9 Represented certificated employees are not allowed to install software or applications onto  
10 computers, the computer network, or any District technology systems without a valid purchase  
11 order or other proof of District or personal ownership. Legal software and/or data stored on  
12 District technology devices are subject to removal with prior notification and consent of the  
13 represented certificated staff member. Long Beach Unified School District shall take  
14 reasonable precautions to ensure the security, integrity, or longevity of data and/or programs  
15 stored on District technology systems.  
16

17 Represented certificated staff acknowledge that they share responsibility for any and all use of  
18 the District's technology systems and that misuse could lead to liability and/or consequences  
19 that extend beyond the District's authority. The Long Beach Unified School District and its  
20 represented certificated staff members shall be held harmless from any use or misuse of District  
21 technology systems by students. Long Beach Unified School District makes no warranty of  
22 any kind, whether expressed or implied, for the service that it is providing. Long Beach  
23 Unified School District will not be responsible for any damage users may suffer including, but  
24 not limited to, loss of data or interruptions of service as a consequence of equipment failure,  
25 either on or off District property. Long Beach Unified School District and its represented  
26 certificated employees are not responsible for the accuracy or quality of the information  
27 obtained through or stored on the system.  
28  
29  
30

31 Ratified 01.05.2016  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46