

## APPENDIX F

### District Technology Internet 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 communications  
4 on those networks. Users shall comply with District standards and will abide by the policies  
5 specified herein. Violations of the District policy described may result in access privileges being  
6 suspended or revoked, as well as other disciplinary action as warranted. Any commercial,  
7 political, or unauthorized use of District technology systems or services, in any form, is forbidden.  
8 All copyright laws must be observed.

9  
10 Members of the certificated teachers bargaining unit may engage in teacher association business  
11 on the District computer networks. Such teacher association business shall be conducted during  
12 non-duty hours which are defined in Article IV, Section C of this Agreement. Association use of  
13 District e-mails shall be limited to the following: authorized Association representatives may use  
14 District e-mails to provide notice of meetings, agendas for meetings, minutes of meetings,  
15 confirmation of a meeting with a District representative, or a limited distribution communique`  
16 between an authorized Chapter officer and a District representative; the Association will not use  
17 e-mail to denigrate the District or its personnel and will observe the prohibitions of Education  
18 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 suspected  
23 either of disrupting or endangering the security or integrity of any District technology systems or  
24 services or of violations of applicable school district policies, federal or state law. Even then, the  
25 system administrator must normally obtain prior approval of the Executive Director of Information  
26 Services or the Deputy Superintendent of Education Services unless grave danger to the continued  
27 operation of the District's technology systems requires emergency action.

28  
29 This does not preclude Technology and Information Services staff from maintaining and  
30 monitoring system logs of user activity which access District technology systems. Moreover,  
31 automated searches for activities that endanger system security or integrity are preformed regularly  
32 to protect all users. Technology and Information Services administrators may take appropriate  
33 action in response to detection of such activity (typically removal of infected files and possibly  
34 suspension of the user's accounts until the matter can be resolved).

35  
36 Use of District technology systems may be revoked at any time for inappropriate use. The  
37 Technology and Information Services Branch, in collaboration with school administration, will be  
38 the sole determiners of what constitutes inappropriate behavior according to local, state, and  
39 federal law. The violation of any item contained in this policy may result in the loss of access  
40 and/or to District technology systems other disciplinary action, as well as possible punitive action  
41 as provided for by local, state, and federal law.

42  
43 The security of any information system is a high priority, especially any system that has many  
44 users and/or Internet access. Represented certificated staff members shall not let others use his or  
45 her account or password as he or she has a reasonable responsibility for all actions related to his  
46 or her account. Certificated staff must notify school administrators immediately if their password

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

7  
8 Represented certificated employees are not allowed to install software or applications onto  
9 computers the computer network, or any District technology systems without a valid purchase  
10 order or other proof of District or personal ownership. Legal software and/or data stored District  
11 technology devices are subject to removal with prior notification and consent of the represented  
12 certificated staff member. Long Beach Unified School District shall take reasonable precautions  
13 to ensure the security, integrity, or longevity of data and/or programs stored on District technology  
14 systems.

15  
16 Represented certificated staff acknowledge that they share responsibility for any and all use of the  
17 District’s technology systems and that misuse could lead to liability and/or consequences that  
18 extend beyond the District’s authority. The Long Beach Unified School District and its  
19 represented certificated staff members shall be held harmless from any use or misuse of District  
20 technology systems by students. Long Beach Unified School District makes no warranty of any  
21 kind, whether expressed or implied, for the service that it is providing. Long Beach Unified School  
22 District will not be responsible for any damage users may suffer including, but not limited to, loss  
23 of data or interruptions of service as a consequence of equipment failure, either on or off District  
24 property. Long Beach Unified School District and its represented certificated employees are not  
25 responsible for the accuracy or quality of the information obtained through or stored on the system.

26  
27  
28  
29 CDC/HS Ratified 01.05.16  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46