



TWIN VALLEY SCHOOL DISTRICT

4851 N. Twin Valley Road · Elverson, PA 19520

Telephone: 610-286-8600 · Fax: 610-286-8608

No: 815

SECTION(S): Operations

TITLE: Acceptable Use of

Internet/Electronic Resources

ADOPTED: February 20, 2001

REVISED: April 17, 2023

1		No. 815 - Acceptable Use of Internet/Electronic Resources	1
2			2
3			3
4	1. Purpose	The TWIN VALLEY SCHOOL DISTRICT provides employees, students, School Board Members, and guests (users) with approved access to the District's technology resources.	4
5			5
6			6
7			7
8		The Board supports the use of the District's technology resources for educational purposes and to carry out the legitimate business and operation of the District.	8
9			9
10			10
11			11
12		Any unauthorized third-party usage of the District's technology resources is prohibited.	12
13			13
14			14
15		The use of the District's technology resources shall be consistent with the curriculum adopted by the District and made available for the performance of job duties consistent with the educational mission of the District. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules and must not cause damage to the District's technology resources.	15
16			16
17			17
18			18
19			19
20			20
21		All employees and students are responsible for the appropriate and lawful use of the District's technology resources.	21
22			22
23			23
24			24
25		<u>Child Pornography</u> is prohibited, see Act 47 U.S.C. § 254; and Act 24 P.S. § 4601	25
26			26
27			27
28		<u>District Technology Resources</u> - All technology owned, operated, and/or licensed by the District.	28
29			29
30			30
31		<u>Educational Purpose</u> - Use that is consistent with the curriculum adopted by the District as well as the varied instructional needs of students.	31
32			32
33	2. Definitions	<u>User(s)</u> - Anyone who utilizes or attempts to utilize District technology resources while on or off District property.	33
34			34
35			35
36			36
37	3. Authority	The District does not guarantee accuracy, endorse, or accept responsibility for information that is retrieved via the Internet. The District shall not be responsible for electronic information that may be lost, damaged, or unavailable. The District shall not be responsible for any unauthorized charges or fees.	37
38			38
39			39
40			40
41			41
42		The Board establishes that network use is a privilege, not a right; Inappropriate, unauthorized and illegal use will result in cancellation of those privileges as well as appropriate disciplinary action. The District provides	42
43			43
44			44

1		these resources for educational and operational purposes as stated herein	1
2		and are not provided as a public access service.	2
3			3
4		While using District-owned devices, users must utilize the District's networks	4
5		for access to the internet while on school property. Other means of access	5
6		are not permitted (e.g. WIFI hotspots, personal internet access, open/rogue	6
7		networks etc.).	7
8			8
9		The District will implement internet and network safety measures through	9
10		policy, guidelines and the use of filtering technology to monitor access by	10
11		minors.	11
12			12
13		The Superintendent or designee shall develop procedures, in cooperation	13
14	4. Delegation of	with the District technology staff, for the acceptable use of all District	14
15	Responsibility	technology resources.	15
16			16
17		<u>Use of Personal Electronic Devices</u> - see SB Policy 237	17
18	5. Guidelines		18
19		<u>Unauthorized Use Prohibited</u> - Only users who have agreed to abide by the	19
20		terms of this policy may utilize the District's technology resources.	20
21		Unauthorized use, utilizing another user's District account, or exceeding	21
22		one's authorization to use District technology resources is prohibited.	22
23		Sharing user credentials and/or passwords between users is strictly	23
24		prohibited.	24
25			25
26		<u>Privacy</u> - The District reserves the right to monitor any user's utilization of	26
27		District technology resources. Users have no expectation of privacy while	27
28		using District technology resources whether on or off District property. The	28
29		District may monitor, inspect, copy, and review any and all usage of District	29
30		technology resources including information transmitted and received via the	30
31		internet to ensure compliance with this and other District policies,	31
32			32
33		and state and federal law. All emails and messages, as well as any files	33
34		stored on District technology resources may be inspected at any time for any	34
35		reason. The District may decrypt and inspect encrypted Internet traffic and	35
36		communications to ensure compliance with this policy.	36
37			37
38		<u>Filtering and CIPA Compliance</u> - The District reserves the right to restrict	38
39		access to any internet site or resource. As required by law, the District shall	39
40		utilize content and messaging filters designed to prevent users from	40
41		accessing materials deemed obscene, offensive, pornographic, harmful to	41
42		minors. Such restrictions will apply to all District devices and users.	42
43			43
44		<u>Monitoring</u> - District technology resources shall be monitored to ensure	44
45		compliance with this and other District policies including monitoring of users'	45
46		online activities. The Superintendent or designee will not use District	46
47		technology to physically track students or devices while not on District	47
48		property except where necessary to recover lost or stolen District technology.	48
49			49
50		<u>District Provided Resources</u> - District technology resources may be assigned	50
51		to an individual user despite being assigned to a particular user, the	51
52		technology resources remain the property of the District and may be	52
53		revoked, suspended, or inspected at any time. Users of District technology	53

1		are responsible for maintaining proper care of the hardware assigned to	1
2		them by the District. If the user shows negligence toward District equipment,	2
3		fees may be applied to the user.	3
4			4
5		<u>Social Media and Networking</u> - The District is not responsible for, nor does it	5
6		endorse messages, narratives or rhetoric published by users whose content	6
7		is inconsistent with the educational purpose of the District. In addition, users	7
8		shall not publish or post information deemed confidential or non-public. See	8
9		SB Policy 815.3.	9
10			10
11		<u>Incidental Personal Use</u> - Occasional personal use by an individual must	11
12		comply with this policy and all other policies, procedures, and rules, must be	12
13		outside of their established work hours, and may not interfere with the	13
14		employee's duties or the educational purpose of the District.	14
15			15
16	6. Prohibitions	The following uses of District technology resources are prohibited, but not	16
17		limited to:	17
18			18
19		1. Use of technology resources to violate the law, facilitate illegal	19
20		activity, or to encourage others to do so.	20
21			21
22		2. Use of technology resources to violate any other District policy.	22
23			23
24		3. Use of technology resources to engage in any intentional act which	24
25		might threaten the health, safety, or welfare of any person or persons.	25
26			26
27		4. Use of technology resources to cause, or threaten to cause mental or	27
28		physical harm to others or damage to their property.	28
29			29
30		5. Use of technology resources to bully, or to communicate terroristic	30
31		threats, discriminatory remarks, or hate.	31
32			32
33		6. Use of technology resources to create, access, distribute, or	33
34		communicate words, photos, videos, or other depictions that are	34
35		obscene, indecent, vulgar, rude, profane, pornographic, harassing,	35
36		terroristic materials, firearms, or illegal drug use.	36
37			37
38		7. Use of technology resources to attempt to interfere with or disrupt	38
39		District technology systems, networks, services, or equipment including,	39
40		but not limited to, the propagation of computer "viruses" and/or	40
41		"malware".	41
42			42
43		8. Altering or attempting to alter other users' credentials or system files,	43
44		system security software, system or component settings, or the systems	44
45		themselves without authorization.	45
46			46
47		9. The attempted physical harm or attempted destruction of District	47
48		technology resources.	48
49			49
50		10. Use that conceals or attempts to conceal a user's identity, including	50
51		the use of anonymizers, or the impersonation of another user.	51
52			52
53		11. Unauthorized access, interference, possession, or distribution of	53

1		confidential or private information.	1
2			2
3		12. Use of technology resources to commit plagiarism.	3
4			4
5		13. Installing, loading, copying, or running software programs,	5
6		applications, or utilities not explicitly authorized by the District	6
7		technology staff.	7
8			8
9		14. Installing unauthorized computer hardware, peripheral devices,	9
10		network hardware, or system hardware onto technology resources,	10
11		including but not limited to plugging into ethernet jacks.	11
12			12
13		15. The use of proxies or other means to bypass Internet content filters	13
14		and monitoring.	14
15			15
16		16. Unauthorized access into a restricted system or changing settings or	16
17		access rights to a restricted system or account.	17
18			18
19		17. Sending unsolicited mass-email messages, also known as spam.	19
20			20
21		18. Scanning the District's technology resources for security	21
22		vulnerabilities.	22
23			23
24	7. Consequences	Violations of this policy may result in the temporary or permanent revocation	24
25		of a user's right to access District technology resources. Additionally, users	25
26		may be subject to other forms of disciplinary actions for violations of this	26
27		policy and/or local, state, and federal law.	27
28			28
29	8. Limitation of	The District makes no guarantees of any kind, whether express or implied,	29
30	Liability	for the service it is providing through its various technology resources. The	30
31		District is not responsible, and will not be responsible, for any damages,	31
32		including loss of data resulting from delays, non-deliveries, missed	32
33		deliveries, or services interruption. Use of any information obtained through	33
34		the District's technology resources is at the user's own risk. To the extent	34
35		permitted by local, state, and federal law, users of District technology	35
36		resources shall indemnify, defend, and hold harmless the District from any	36
37		actions, claims, lawsuits, penalties, fines, or similar sanctions brought	37
38		against the District in connection with a user's improper or unauthorized use	38
39		of District technology resources.	39
40			40
41		<u>References:</u>	41
42			42
43		18 USC 2256 <i>Harmful materials definitions</i>	43
44			44
45		18 PA CSA 6312 <i>Sexual abuse of children</i>	45
46			46
47		20 USC 6777 <i>Internet safety</i>	47
48			48
49		18 PA CSA 5903 <i>Obscene and other sexual materials and performances</i>	49
50			50
51		24 PS 4604 <i>School entity Internet policies</i>	51
52			52
53		24 PS 4610 <i>School entity Internet Disabling blocking technology for use by</i>	53

1		<i>certain persons</i>	1
2			2
3		47 U.S.C. § 254; and Act 24 P.S. § 4601 <i>Children's Internet Protection Act</i>	3
4			4
5		SB Policy 237	5
6			6
7		SB Policy 815.3	7
8			8
9			9
10			10
11			11
12			12
13			13
14			14
15			15
16			16
17			17
18			18
19			19
20			20
21			21
22			22
23			23
24			24
25			25
26			26
27			27
28			28
29			29
30			30
31			31
32			32
33			33
34			34
35			35
36			36
37			37
38			38
39			39
40			40
41			41
42			42
43			43
44			44
45			45
46			46
47			47
48			48
49			49
50			50