

DISCOVERY CHARTER SCHOOL BOARD OF TRUSTEES MEETING AGENDA

February 27, 2023 5:00-6:30 p.m.

Location for Public Meeting: 133 Hoover Drive, Rochester NY 14615

Remote Attendance for Public Meeting Option: Zoom Link

The meeting information was included in Public Notice as well as on the school's website:

**Topic: Discovery Charter School- Board of Trustees Meeting
2.27.2023**

5:00 PM Eastern Time (US and Canada)

Zoom link:

<https://us06web.zoom.us/j/86450663136?pwd=RkdPU3dTRGJmNkFzKy9CUlc2Nys0QT09>

Meeting ID: 864 5066 3136

Passcode: Discovery

1. Call to Order
2. Proof of Public Notice of Meeting
3. Conflict of Interest Reminder
4. Public Comment
5. Consent Agenda: Approve Minutes for Meeting of 1-26-2023
6. Committee Reports
 - a. Audit & Finance Committee Report—Minutes included in Board Materials
 - b. Governance Committee Report
 - c. Executive Committee Report
 - d. Academic Excellence Committee
 - e. Personnel Committee Report
 - f. Committee on Diversity, Equity, and Inclusion Report
 - g. Parent Representative Report
7. School Director Report (Community Circle, ELA Benchmarks)
8. NYS Comptroller Report on Network and Financial Software Controls
9. Executive Session: School Director Evaluation: Mid-year check-in
10. Motion to Adjourn (*Action Required*)

Next Regular Meeting: TBD

DISCOVERY CHARTER SCHOOL BOARD OF TRUSTEES

MEETING MINUTES

January 26, 2026; 5:30 P.M.

133 Hoover Drive, Rochester, New York 14615

Physical Location for Public Meeting: 133 Hoover Drive, Rochester NY 14615 (School Director's Office)

Remote Attendance for Public Meeting Option: Zoom Link

The meeting information was included in Public Notice as well as posted at the school and on the website

Topic: Discovery Charter School- Board of Trustees Meeting 1.26.2023

Time: January 26, 2023 5:30 PM Eastern Time (US and Canada)

Join Zoom Meeting

<https://us06web.zoom.us/j/86450663136?pwd=RkdPU3dTRGJmNkFzKy9CUlc2Nys0QT09>

Meeting ID: 864 5066 3136

Passcode: Discovery

Trustees Present: L. Lewis (Vice Chair), S. Adair (Treasurer), R. Stiles, E. Stubbs, C. Wilkins, S. Fazili, Marisol Galarza-Ruiz

Trustee Participating Remotely: S. Varhus (Chair)

Trustees Excused: D. Braveman

Also Present: S. Castner (School Director), M. Bradstreet (Data Coordinator), K. Snyder (Assistant School Director)

Participating Remotely: A. Culver (Finance Manager), J. Stanberry (Administrative Intern)

1. Call to Order

- a. The Chair called the meeting to order at 5:34, and it was determined that a lawful quorum of six was present.

2. Proof of Public Notice of Meeting

- a. Public Notice was provided in the *Democrat and Chronicle*, posted at the school and on the school website

3. Conflict of Interest Reminder

- a. The Chairperson read the following statement: “The Chair reminds everyone that, if a potential conflict of interest exists concerning a subject under discussion by the Board, you have an obligation to disclose the potential conflict and, if deemed a conflict, recuse yourself and leave the room during any discussion and vote on the subject.”

4. Opportunity for Public Comment: no public comment

5. Welcome and Introduction- Marisol Galarza-Ruiz: new trustee, will be starting orientation soon

6. Consent Agenda: Approve Minutes for Meeting of 12.20.2022 with addition of S. Fazili to attendance- Moved by S. Adair, seconded by C. Wilkins, approval was unanimous.

7. Committee Reports

- a. Executive Committee: *(no report)*
- b. Academic Excellence Committee: Met, minutes were distributed, discussed iReady data, computer based state tests coming soon, fifth grade science test in 2024, idea of devoted science teacher for next year.

- c. Governance Committee Report: *(no report)*
- d. Personnel Committee Report: *(no report, will meet in February)*
- e. Audit & Finance Committee Report: Met, minutes were distributed, the financial outlook is promising, trending in a favorable direction at this time.
- f. Ad Hoc Committee on Diversity, Equity & Inclusion: *(no report)*
- g. Parent Representative Report: Transition to new Family Liaison, upcoming family associate meeting 2/7/23

8. School Director Report: S. Castner shared iReady data, improvement is seen as far as more students who are on grade level and students who have moved up. The math benchmark, which will be a good predictor of state test scores, is scheduled for 3/14. Rigby reading data also shows improvement, including cohorts (ex. 1st graders who are now 2nd graders). ELA benchmark is scheduled for 2/7. For a professional development opportunity, S. Castner has applied to the Leverage Leadership Institute, a highly selective Fellows program looking for school leaders who have led their schools to high achievement and great improvement.

9. Revised Resolution #480: Key Design Elements *(action required)* Moved by R. Stiles, seconded by S. Adair, unanimously approved.

10. IT Audit and IT Policies: Resolution #482, approving Policies #5100, #5110, #5120, #5130 *(action required)* These policies were recommended from the state audit, moved by S. Adair, seconded by E. Stubbs, approved unanimously.

11. Adjournment: C. Wilkins moved and R. Stiles seconded a motion to adjourn; the motion was approved unanimously.

Next Regular Meetings: **Friday Feb 10, 2023**

Minutes submitted by M. Bradstreet

Finance Committee Meeting Minutes
Meeting Date 02/09/2023 / Time: 8:00 am
Minutes Recorded By: Anne Culver

Committee Chair:	Scott Adair		
Committee Members	Name	Present	Excused
	Sara Varhus		X
	Scott Adair	X	
	Sareer Fazili		X
	Sara Castner	X	
	Kara Snyder	X	
	Anne Culver	X	

MEETING AGENDA, MINUTES AND ACTION ITEMS			
Agenda Item	Discussion	Action Item	Responsible Party
Financial Statement Review	The January balance sheet and profit and loss were reviewed. No significant changes from last month and DCS is on track financially. The revised budget was reviewed. We are no longer expecting a significant loss, but instead will have a small profit. Preliminary 23-24 FY budget preparations will begin soon and will include 20 additional students per the charter revision. 23-24 FY Budget expected to be brought to the board in April.	2023-24 Preliminary Budget	Anne Culver, Sara Castner, Kara Snyder

Finance Committee Meeting Minutes
Meeting Date 02/09/2023 / Time: 8:00 am
Minutes Recorded By: Anne Culver

DISCOVERY CHARTER SCHOOL Budget

	2019-20 Actual	2020-21 Budget	2021-22 Actual	2022-23 Budget Approved	2022-23 Revised Budget	2022-23 YTD thru 01/31/23	Budget % Change
Income						58% thru FY	
410-010 Per Pupil Allocation Income	\$ 3,858,269	\$ 3,780,021	\$ 3,827,209	\$ 4,100,000	\$ 4,000,000	\$ 2,304,355	
410-025 High Cost Aid	435,510	350,000	180,345	200,000	175,000	96,827	
450-050 Federal IDEA	23,349	31,626	37,357	37,356	37,090	37,090	
450-030 Title I A&D	142,920	166,000	169,897	186,000	212,719	58,819	
450-020 Title II A	11,769	33,949	23,962	23,900	24,516	4,903	
450-035 Title IV	5,103	33,949	13,106	13,000	13,701	2,740	
CRRSA Act Funding	-	166,173	320,939	-	261,820	126,972	
ARP Act Funding	-	-	427,216	630,000	368,180	277,742	
CARES Act	-	-	-	-	132,939	132,939	
415-010 Contributions and donations	2,184	-	2,951	-	791	791	
415-020 Miscellaneous	1,033	-	2,534	-	275	274	
410-020 Food Service Income	197,245	60,000	362,240	334,668	325,000	180,315	
425-010 Uniform Income	-	-	-	-	440	440	
450-040 Fresh Fruits & Veg Programs	9,376	18,000	24,892	16,800	16,800	8,607	
490-010 - PPP Loan Forgiveness	-	-	-	-	-	-	
Other Grants	-	10,000	-	-	66,350	51,350	
E-rate Reimbursement	-	32,886	10,862	18,298	3,530	3,530	
In-Kind District Textbooks	-	163,310	16,427	17,687	-	-	
TOTAL INCOME	\$ 4,686,758	\$ 4,698,914	\$ 5,419,937	\$ 5,577,711	\$ 5,656,838	\$ 3,287,694	4.4%
Actual YTD Income vs Full Year Budget							
Expense							
520-010 Salaries & Wages	\$ 2,995,681	\$ 2,354,525	\$ 3,451,359	\$ 3,233,318	\$ 3,185,000	\$ 1,675,036	
525-045 HSA Employee Contribution	-	-	9,000	9,000	-	-	
525-016 Vision Insurance	-	-	2,304	4,067	2,500	1,063	
525-017 Dental Insurance	-	-	18,891	12,561	18,000	11,039	
525-010 FICA	-	-	246,812	247,381	244,000	124,667	
525-015 Health Insurance	-	-	255,734	380,000	225,000	156,713	
525-020 NYSS Disability	-	-	4,520	13,333	4,600	3,076	
525-021 Disability - Supplemental	-	-	2,389	10,643	2,700	1,733	
525-030 Life Insurance	-	-	2,834	15,342	3,000	2,365	
525-025 Retirement Expense	-	-	225,466	282,326	227,000	164,689	
525-035 Workers Compensation Insurance	-	-	26,433	23,000	26,000	17,110	
525-040 Unemployment Insurance Expense	-	-	31,281	22,148	30,000	14,249	
Total 525 - Employee Benefits	816,482	787,212	826,664	1,019,801	791,800	495,704	
Total Personnel Expense	3,812,163	3,141,737	4,278,023	4,253,119	3,976,800	2,170,740	-7.0%
Actual YTD Personnel Exp vs Full Year Budget							
530 - School Operations							
540-115 Mixer Equipment/Furniture	6,132	8,000	20,248	40,000	30,000	14,423	
530-053 Transportation	12,619	10,000	5,042	10,000	40,000	36,103	
530-120 Yearbook	97	2,000	-	2,000	3,091	3,091	
530-105 Miscellaneous Expense	1,303	-	2,889	-	500	258	
530-005 Office Supplies	16,911	18,000	22,737	20,000	18,000	7,069	
530-010 Classroom Supplies	25,768	26,000	28,168	36,000	36,000	21,093	
530-015 Special Education Supplies	205	2,500	-	3,500	1,500	302	
530-025 Food Service Supplies	1,309	3,000	1,807	5,000	2,200	1,024	
530-030 Postage	2,610	2,500	402	2,500	750	213	
530-035 Printing/Copying	6,754	15,000	8,085	22,500	6,000	(1,437)	
530-040 Telephone	14,357	17,500	17,614	17,500	18,000	11,391	
530-045 Marketing & Advertising	8,670	9,000	7,992	9,000	9,000	4,651	
530-055 Travel	1,503	4,000	373	4,000	2,000	828	
530-060 Professional Development Exp	12,305	13,000	9,878	15,000	15,000	6,182	
530-070 Board Expense	809	850	887	850	850	-	
530-075 Expedition	3,103	13,500	-	-	1,500	707	
530-080 Staff Recruitment & Retention	-	-	-	-	6,500	5,003	
530-085 Textbooks	5,869	25,000	86,587	40,000	35,000	10,558	
530-120 Student Uniforms	-	2,500	6,627	4,000	4,000	2,100	
530-070 Computer Supplies & Software	24,465	100,000	74,249	100,000	75,000	15,340	
530-065 Meeting Expense	1,307	1,500	1,322	1,500	1,500	-	
530-050 Dues and Subscriptions	10,602	10,600	1,615	10,600	5,500	5,341	
530-095 Student Testing	5,404	6,500	19,602	6,500	20,000	14,120	
Total 530 - School Operations	163,102	290,950	316,124	350,450	331,891	158,560	5.0%
Actual YTD School Op Exp vs Full Year Budget							
540 - Contracted Services							
540-005 Auditing	18,000	18,000	16,156	22,000	26,669	26,670	
540-006 Accounting Services	10,304	10,000	7,155	12,000	1,140	1,140	
540-045 Other Purchased Prod/Consult	86,796	40,000	4,750	32,000	20,000	11,693	
540-040 Enrichment - After School	-	-	1,844	-	-	-	
540-041 Enrichment - Summer Learning	-	20,000	27,919	100,000	25,000	138	
540-010 Legal Fees	14,469	14,000	25,586	20,000	20,000	8,548	
540-012 Landlord - Admin Services	97,434	99,250	90,922	90,000	96,424	67,341	
540-015 Expeditionary Learning Fees	7,500	-	-	-	-	-	
540-025 Food Service Fees	181,827	60,000	307,123	315,000	315,000	186,796	
540-030 Payroll Processing	2,801	3,800	3,997	4,500	18,000	3,992	
Total 540 - Contracted Services	419,131	265,150	489,452	595,500	522,133	306,318	6.7%
Actual YTD Contracted Svcs Exp vs Full Year Budget							
550 - Facility Operation							
550-005 Insurance	28,212	30,679	39,867	52,000	43,000	26,140	
550-010 Janitorial	-	-	126,102	-	151,000	91,018	
550-015 Maintenance & Repairs	7,687	8,000	13,198	114,000	5,000	1,880	
550-021 Facility Lease - Hoover	433,890	433,886	361,377	363,000	362,000	210,742	
550-050 Utilities	39,084	50,000	68,165	55,000	68,000	24,361	
550-055 Property Taxes	-	1,326	671	3,000	1,000	-	
550-030 Equipment Lease	8,820	11,000	9,163	10,000	10,000	5,282	
Total 550 - Facility Operation	518,693	1,153,434	618,543	595,000	640,000	359,423	3.5%
Actual YTD Facility Op Exp vs Full Year Budget							
Other							
560-090 Fraud Expense	-	-	-	-	-	-	
550-090 Depreciation	139,418	93,667	110,787	108,000	111,620	56,252	0.8%
Contingency	-	-	-	25,000	-	-	
TOTAL EXPENSE	5,052,507	4,944,938	5,812,929	5,827,069	5,582,544	3,051,193	-4.0%
Actual YTD Expense vs Full Year Budget							
NET OPERATING SURPLUS/(DEFICIT)	\$ (365,749)	\$ (246,024)	\$ (392,992)	\$ (349,358)	\$ 74,294	\$ 236,401	

DISCOVERY CHARTER SCHOOL
Profit/Loss YTD Comparison w/Budget
As of November 30, 2022

	Actual Month 01/31/2023	Actual YTD 01/31/2023	Actual YTD 01/31/2023	Actual YTD 01/31/2023	Actual YTD Special Aid Fund	Actual YTD 01/31/2023	PRIOR YTD 01/31/2022	Budget Full Year	Remaining Budget \$	% Used/ Received of Budget
Income										
410-010 Per Pupil Allocation Income	\$ 401,140	\$	2,304,355			2,304,355	\$ 2,320,362	\$ 4,100,000	\$ 1,795,645	58%
410-025 High Cost Aid	-		96,827			96,827	116,832	200,000	103,173	56%
450-050 Federal IDEA	-		-		37,090	37,090	-	37,358	268	48%
450-030 Title I A&D	-				58,819	58,819	37,230	186,000	127,181	99%
450-020 Title IIA	-				4,903	4,903	4,792	23,900	18,997	32%
450-035 Title IV	-				2,740	2,740	2,621	13,000	10,260	21%
450-090 CARES Act	-				132,939	132,939	-	-	(132,939)	21%
450-105 CRRSA ESSER 2	-				126,972	126,972	116,551	630,000	(126,972)	44%
450-100 ARP ESSER 3	-				277,742	277,742	-	-	352,258	0%
415-010 Contributions and donations	-		791			791	475	-	(791)	0%
415-020 Miscellaneous	-		274			274	2,500	-	(274)	0%
410-020 Food Service Income	36,124	180,315	-			180,315	130,308	334,668	154,353	54%
410-120 Child Nutrition Emergency Fund	-					-	50,588	-	-	
450-040 Fresh Fruits & Veg Programs	-	8,607	-			-	10,393	16,800	-	
450-080 Other Grants	-					-	-	-	-	
450-110 COVID Response - Remote	-				8,000	8,000	-	-	(8,000)	0%
425-010 Uniform Income	-		440		43,350	43,350	-	-	(43,350)	0%
415-025 E-rate Reimbursement	-		3,530			3,530	1,505	-	(440)	0%
415-015 In-Kind District Textbooks	-					-	-	18,298	14,768	19%
TOTAL INCOME	\$ 437,264	\$ 188,922	\$ 2,406,217	\$ 692,555	\$ 3,287,694	\$ 2,794,157	\$ 5,577,711	\$ 2,467,618		
Expense										
520-010 Salaries & Wages	\$ 263,824	\$ 11,427	\$ 1,108,308	\$ 555,301	\$ 1,675,036	\$ 1,756,205	\$ 3,233,318	\$ 1,558,282		52%
525-045 · HSA Employee Contribi	-		-			-	-	-	-	
525-016 Vision Insurance	157		1,063			1,063	1,476	-	-	
525-017 · Dental Insurance	1,599		11,039			11,039	11,867	-	-	
525-010 · FICA	19,436		124,667			124,667	130,450	-	-	
525-015 · Health Insurance	19,477		156,713			156,713	156,375	-	-	
525-020 · NYS Disability	(156)		2,076			2,076	3,386	-	-	
525-021 · Disability - Supplementi	345		1,733			1,733	1,451	-	-	
525-030 · Life Insurance	212		2,365			2,365	1,940	-	-	
525-025 Retirement Expense	23,527		164,689			164,689	131,163	-	-	
525-035 · Workers Compensation	5,716		17,110			17,110	17,105	-	-	
525-040 · Unemployment Insuranc	11,309		14,249			14,249	16,062	-	-	
Total 525 · Employee Benefits	81,622	-	495,704	-	495,704	471,275	1,019,801	524,097		49%
Total Personnel Expense	345,446	11,427	1,604,012	555,301	2,170,740	2,227,480	4,253,119	2,082,379		
Actual YTD Personnel Exp vs Full Year Budget										
530 · School Operations										
540-115 · Minor Equipment/Furni	266	2,184	12,239			14,423	17,490	40,000	25,577	36%
530-053 · Transportation	-		36,103			36,103	3,336	10,000	(26,103)	361%
530-120 · Yearbook	-		3,091			3,091	-	2,000	(1,091)	155%

As of November 30, 2022

	Actual Month 01/31/2023	Actual YTD 01/31/2023	Actual YTD Operating Fund	Actual YTD 01/31/2023 Special Aid Fund	Actual YTD TOTAL	PRIOR YTD 01/31/2022 TOTAL	Budget Full Year	Remaining Budget \$	% Used/ Received of Budget
530-105 · Miscellaneous Expense	-	258	258		258	1,828	-	(258)	
530-005 · Office Supplies	314	7,069	7,069		7,069	13,153	20,000	12,931	35%
530-010 · Classroom Supplies	1,123	18,880	18,880	2,213	21,093	20,640	36,000	14,907	59%
530-015 · Special Education Supplies		302	302		302	-	3,500	3,198	9%
530-025 · Food Service Supplies		1,024	-		1,024	897	5,000	3,976	20%
530-030 · Postage		213	213		213	198	2,500	2,287	9%
530-035 · Printing/Copying	890	(1,437)	(1,437)		(1,437)	4,443	22,500	23,937	-6%
530-040 · Telephone	620	11,391	11,391		11,391	9,377	17,500	6,109	65%
530-045 · Marketing & Advertising		4,651	4,651		4,651	2,385	9,000	4,349	52%
530-055 · Travel		828	828		828	373	4,000	3,172	21%
530-060 · Professional Developme	68	211	5,371	600	6,182	6,634	15,000	8,818	41%
530-070 · Board Expense		-	-		-	-	850	850	0%
530-075 · Expedition		707	707		707	-	-	(707)	
530-085 · Textbooks	77	2,934	2,934	7,624	10,558	110,203	40,000	29,442	26%
530-080 · Staff Recruitment & Ret	48	4,645	4,645	358	5,003	-	-	(5,003)	
530-120 · Student Uniforms		2,100	2,100		2,100	(2,060)	4,000	1,900	53%
530-020 Computer Supplies & Sof	603	13,797	13,797	1,543	15,340	33,376	100,000	84,660	15%
530-065 Meeting Expense					-	2,200	1,500	1,500	0%
530-050 Dues and Subscriptions		5,341	5,341		5,341	1,264	10,600	5,259	50%
530-095 · Student Testing		14,320	14,320		14,320	18,103	6,500	(7,820)	220%
Total 530 · School Operations	4,009	3,419	142,803	12,338	158,560	243,840	350,450	191,890	
Actual YTD School Op Exp vs Full Year Budget									
540 · Contracted Services							45%		
540-005 - Auditing	-	26,670	26,670		26,670	16,156	22,000	(4,670)	121%
540-006 - Accounting Services	-	1,140	1,140		1,140	4,035	12,000	10,860	10%
540-045 - Other Purchased/Prof/C	7,558	11,693	11,693		11,693	3,875	32,000	20,307	37%
540-040 · Enrichment - After School		-	-		-	1,844	-	-	
540-041 · Enrichment - Summer Learning		138	138		138	27,919	100,000	99,862	0%
540-010 · Legal Fees	1,265	8,548	8,548		8,548	19,436	20,000	11,452	43%
540-012 · Landlord - Admin Servit	7,271	67,341	67,341		67,341	53,038	90,000	22,659	75%
540-025 · Food Service Fees	31,280	186,796	-		186,796	136,912	315,000	128,204	59%
540-030 · Payroll Processing	2,516	3,992	3,992		3,992	1,391	4,500	508	89%
Total 540 · Contracted Services	49,890	186,796	119,522	-	306,318	264,606	595,500	289,182	
Actual YTD Contracted Svcs Exp vs Full Year Budget									
550 · Facility Operation							51%		
550-005 · Insurance	4,059	26,140	26,140		26,140	21,680	52,000	25,860	50%
550-015 · Maintenance & Repairs	-	1,880	1,880	\$	1,880	10,900	4,000	2,120	47%
550-015 · Janitorial	14,027	91,018	91,018	\$	91,018	74,013	110,000	18,982	83%
550-021 · Facility Lease - Hoover	30,106	210,742	210,742		210,742	204,604	362,000	151,258	58%
550-050 Utilities	-	24,361	24,361		24,361	32,824	55,000	30,639	44%

DISCOVERY CHARTER SCHOOL
Profit/Loss YTD Comparison w/Budget
As of November 30, 2022

	Actual Month 01/31/2023	Actual YTD 01/31/2023	Actual YTD 01/31/2023 Food Service Fund	Actual YTD 01/31/2023 Operating Fund	Actual YTD 01/31/2023 Special Aid Fund	ACTUAL YTD 01/31/2023 TOTAL	PRIOR YTD 01/31/2022 TOTAL	Budget Full Year	Remaining Budget \$	% Used/ Received of Budget
550-055 Property Taxes								2,000	2,000	0%
550-030 · Equipment Lease	742			5,282		5,282	5,342	10,000	4,718	53%
Total 550 · Facility Operation	48,934	-	-	359,423	-	359,423	349,363	595,000	235,577	
<i>Actual YTD Facility Op Ex vs Full Year Budget</i>										
								60%		
Other										
560-090 Fraud Expense								-	-	0%
550-090 · Depreciation	-	671		55,581		56,252	56,334	108,000	51,748	52%
Contingency						-	-	25,000	25,000	0%
TOTAL EXPENSE	448,279	202,313	2,281,341	567,639	3,051,293	3,141,623	5,927,069	5,927,069	2,875,776	
<i>Actual YTD Expense vs Full Year Budget</i>										
								51%		
NET OPERATING SURPLUS/(DEFICIT)										
	\$ (11,015)	\$ (13,391)	\$ 124,876	\$ 124,916	\$ 236,401	\$ (347,466)	\$ (349,358)			
NET SURPLUS/(DEFICIT)										
	\$ (11,015)	\$ (13,391)	\$ 124,876	\$ 124,916	\$ 236,401	\$ (347,466)	\$ (349,358)			
INCLUDING REVENUE FOR										



Discovery Charter School

Network and Financial Software Access Controls

2022M-156 | February 2023

Contents

Report Highlights	1
Network and Financial Software Access Controls.	2
How Can the Board and Officials Help Ensure There Are Adequate Network and Financial Software Access Controls?	2
The Board and Officials Did Not Ensure There Were Adequate Network and Financial Software Access Control Policies	3
How Should Officials Ensure Network and Financial Software User Account Access Controls Are Adequate?	3
Officials Did Not Adequately Control Network and Financial Software User Account Access	5
How Does a Written Agreement With the IT Service Provider Help Ensure Network and Financial Software Access Controls Are Adequate?	9
The School Did Not Have an Adequate Written Agreement with the School's IT Service Provider	9
Why Should School Officials Provide IT Security Awareness Training?	10
School Officials Did Not Provide IT Security Awareness Training	10
What Do We Recommend?	11
Appendix A – Response From School Officials	12
Appendix B – Audit Methodology and Standards	13
Appendix C – Resources and Services.	15

Report Highlights

Discovery Charter School

Audit Objective

Determine whether Discovery Charter School (School) officials ensured network and financial software access controls were adequate.

Key Findings

School officials did not ensure that network and financial software access controls were adequate. As a result, data and personal, private and sensitive information (PPSI) are at greater risk for unauthorized access, misuse, or loss. In addition to finding sensitive information technology (IT) control weaknesses, which we communicated confidentially to officials, we found that:

- Officials did not adopt adequate network and financial software policies, establish an IT contingency plan, or provide IT security awareness training.
- 18 percent of the School's enabled nonstudent user accounts were not needed, which created additional entry points for someone to inappropriately access the School's network.
- Two of the three financial software user accounts unnecessarily had full access, and three individuals unnecessarily shared access to a user account with administrative permissions. As a result, users could alter data and conceal inappropriate activity with limited ability for officials to trace the activity to a specific user.
- The IT service provider's contract did not define responsibilities. This can contribute to confusion over network responsibilities, which could expose the School's IT assets to risk for unauthorized access, misuse or loss.

Key Recommendations

- Properly manage network and financial software user accounts and establish adequate written policies for network and financial software access.

School officials agreed with our recommendations and indicated they will initiate corrective action.

Background

The School is located in the Town of Greece in Monroe County. The New York State Board of Regents approved the School's charter in December 2010.

The School is governed by an 11-member Board that is responsible for managing and controlling the School's financial and educational affairs. The School Director (Director) is responsible, along with other administrative staff, for the day-to-day management of the School under the direction of the Board.

The School contracts with a vendor to provide IT services, which includes managing network and financial software access controls. The IT service provider assigned three of its employees to the School, including an IT Manager, to provide IT services. The School's Operations Manager is responsible for overseeing the IT service provider.

Quick Facts

Enabled Network User Accounts

Individual Non-Student	86
Service	21
Shared	18
Total	125
Reviewed	125

Financial Software

Enabled User Accounts	3
-----------------------	---

2021-22 IT Service Provider

Agreed Upon Cost	\$90,922
------------------	----------

Audit Period

July 1, 2020 – June 29, 2022

Network and Financial Software Access Controls

The School relies on its network and financial software for maintaining financial, student and personnel records, much of which contain personal, private and sensitive information (PPSI); accessing the Internet; and sending and receiving email. PPSI is any information to which unauthorized access, disclosure, modification, destruction, or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

If the School's network or financial software access is compromised or disrupted, the results could range from inconvenience to significant damage and could require extensive effort and resources to evaluate, repair and/or rebuild. While effective network and financial software access controls will not guarantee the safety of these systems, without these controls the School has an increased risk that its network hardware, financial software and data contained therein, including PPSI, may be exposed, damaged or lost through inappropriate access and use.

How Can the Board and Officials Help Ensure There Are Adequate Network and Financial Software Access Controls?

By adopting written policies and procedures, a charter school (school) board of trustees (board) can help ensure adequate network and financial software access controls. Network and financial software access control policies should describe the tools to use and procedures to follow to help protect these systems and the data they contain, define appropriate user behavior when accessing the network and financial software and explain the consequences of policy violations.

A board should adopt written policies that address user accounts, passwords, remote access and audit trails, which are records of activity indicating who has accessed the network or financial software, the time and date of the access and what activity occurred. A board also must adopt a breach notification policy to ensure that affected parties are notified if unauthorized access of their private information occurs.

In addition, inadequate network and financial software access controls increase the risk of unauthorized access, which could lead to an unexpected disruption. Therefore, a board should adopt a written IT contingency plan containing procedures and technical measures that help enable the recovery of network and financial software operations after an unexpected disruption. The IT contingency plan should address, and establish controls for, how users will access the network and financial software, or its data, as quickly and effectively as possible to maintain school operations.

Without comprehensive written policies and procedures that explicitly convey a school's network and financial software access controls, officials cannot ensure

that users are aware of their responsibilities for helping to protect these systems and the data they contain from unauthorized access, misuse and loss.

The Board and Officials Did Not Ensure There Were Adequate Network and Financial Software Access Control Policies

The Board adopted acceptable use policies that defined appropriate user behavior when accessing the network, but did not adopt other network and financial software access control policies. Specifically, School officials did not develop an IT contingency plan or policies related to:

- User account management, including adding or disabling user accounts on the network or in the financial software.
- Passwords.
- Remote access.
- Audit trails, including requiring officials to review change reports, such as a report of deletions or changes to data.
- Breach notification.

The Director told us that School officials were unaware of the need for these policies and generally relied on the IT service provider to handle all of the School's IT related needs. Without these policies and procedures, the School has an increased risk that its hardware, software and data, including PPSI, may be exposed, damaged or lost through inappropriate access and use.

Also, without a policy requiring regular review of network and financial software audit trails and change reports, officials may not detect unauthorized or inappropriate activity within the network and financial software in a timely manner. In addition, if individuals' private information is improperly accessed, officials may not be able to notify them in a timely manner. Furthermore, without an IT contingency plan, important financial and other data could be lost, or the School could suffer a disruption to operations, which could prevent the School from processing vendor payments and payroll checks.

How Should Officials Ensure Network and Financial Software User Account Access Controls Are Adequate?

School officials are responsible for restricting network and financial software user account access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure that data and IT assets on the network and in the financial software are secure from unauthorized use, modification and/or loss.

Network and financial software user accounts provide access to network resources and financial and employee data and should be actively managed to minimize the risk of unauthorized access and misuse. If not properly managed, unneeded user accounts may not be detected and disabled in a timely manner. Also, unneeded accounts are additional entry points for attackers. If compromised, these accounts could be used to potentially access and view PPSI, make unauthorized changes to accounting records or deny legitimate access to electronic information when needed.

To minimize the risk of unauthorized access, misuse and loss, officials should actively manage network and financial software user accounts and permissions, including their creation, use and dormancy. Officials should disable unneeded user accounts as soon as there is no longer a need for them, and regularly monitor them to ensure they are appropriate and authorized.

Officials should limit the use of service and shared accounts, routinely evaluate the need for them and disable those that are not related to a current school or system need. A service account is an account created for the sole purpose of running a particular network or system service or application (e.g., backups). Service accounts are not linked to individual users and, therefore, may have reduced accountability.

Shared user accounts are accounts with a username and password that are shared among two or more users. Shared accounts are often used to provide access to guests and other temporary or intermittent users (e.g., substitute teachers and third-party vendors). Because shared accounts are not assigned to an individual user, officials may have difficulty managing them and linking any suspicious activity to a specific user.

To help ensure individual accountability, each user should have and use their own user account, when possible. When shared user accounts are provided for temporary work or guests, the accounts should have an expiration date and automatically terminate access after a designated, authorized time period.

Generally, a network administrative account has permissions to monitor and control a network, connected computers and certain applications that can include adding new users and changing user passwords and permissions. A user with network administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. As a result, officials should limit network administrative permissions to those users who need them to complete their job duties and functions.

When financial software is used to process transactions and maintain financial records, school officials should establish adequate access controls that give users access to only those functions that are consistent with their job duties and

responsibilities. Those involved in financial operations should not have access to user accounts with administrative permissions because an individual who has these permissions can generally add new users, configure software settings, override management controls, change user access rights and record and adjust financial transactions.

School officials should ensure that financial software access controls prevent users from being involved in multiple phases of financial transactions, or they should implement effective compensating controls, such as monitoring these users and the transactions that they process.

Officials should ensure that deletions and adjustments cannot be made without authorization and that there is a process in place for an independent party to review data entered into and changed in the software. These actions can help maintain the data's integrity.

Officials Did Not Adequately Control Network and Financial Software User Account Access

School officials did not adequately control network or financial software user account access. As a result, the School had unneeded user accounts, and accounts with unneeded user permissions, that were not disabled, removed or monitored.

We examined all 125 enabled School network user accounts (86 individual nonstudent accounts, 21 service accounts and 18 shared accounts)¹ and all three enabled financial software user accounts to determine whether the accounts and their permissions were needed and adequately controlled. As a result of our review and inquiry, 21 network user accounts (17 percent), including five with administrative permissions, were disabled or deleted, as follows:

Unneeded Individual Network User Accounts – We identified six individual network user accounts that had not been used in at least six months. After we asked School officials to review these accounts, they determined two were necessary and IT service provider staff (IT staff) disabled or deleted² four of the six accounts (67 percent) because they were no longer needed. These user accounts remained enabled much longer than necessary. The disabled and deleted accounts included:

¹ The School did not have any student network user accounts.

² While we typically recommend disabling accounts to preserve a clear audit trail, the IT service provider chose to delete certain accounts. When we discussed this with IT staff, they told us it was generally their practice to initially disable accounts and then delete them after three or more months.

-
- Two for vendor representatives who no longer worked at the School. We found that these user accounts had not been used in more than two years and four years, respectively.
 - One for a former School employee. Although this employee left School employment in June 2020, the network user account remained enabled nearly two years later.
 - One for an individual from an outside organization who never needed a School account. In addition, this account had unneeded administrative permissions.

These accounts should have been disabled as soon as the individuals left School employment or stopped providing services to the School. Generally, these accounts were still enabled because the School's written agreement with its IT service provider did not define expectations related to user account management.

Also, the School did not have adequate procedures for IT staff and School officials to follow to disable accounts. In addition, the IT service provider and School officials did not perform an effective periodic review of authorized users and their access to the network. While IT staff reviewed network user accounts, they did not identify the four unneeded user accounts.

Unneeded Service and Shared Network User Accounts – We found that 14 shared and 12 service network user accounts had not been used in the last six months. After we asked School officials to review these accounts, officials and the IT Manager told us that 12 shared and seven service network user accounts were unneeded.

Of these 19 user accounts, IT staff deleted or disabled 17 (10 shared and all seven service accounts) and allowed two shared user accounts to remain enabled. The IT Manager told us that he would delete the two remaining accounts in the future after further review. Five of these accounts, including one that remained enabled, had administrative permissions.

The Operations Manager and the IT Manager told us that the seven unneeded service accounts were for applications that the School no longer used, and the 10 shared accounts were previously used for various purposes, but were no longer needed. These user accounts remained enabled much longer than necessary. We found that two of these user accounts were not used in more than four years.

The IT Manager also said that the IT service provider performed an annual review of the School's network user accounts to identify any unneeded accounts. However, the IT Manager told us that this review did not include service or shared accounts or user permissions, including administrative permissions.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, possibly could be used to inappropriately access and view School data such as PPSI. When network user accounts are not monitored, compromised accounts may not be detected in a timely manner. In addition, when unneeded user accounts have administrative permissions, the School has an increased risk because the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

Unnecessary Financial Software Permissions – We identified two individual financial software user accounts and a shared account. The two individual user accounts were needed for authorized financial software users: the Operations Manager and the School's financial consultant.

We reviewed the financial software permissions for the two individual accounts to determine whether they were appropriate and adequately controlled. We found that both users' accounts had full access to all financial software modules, which included user permissions to change or delete transactions. Some of these permissions were not needed for these individuals' specific job duties and responsibilities.

In addition, the Operations Manager, assistant operations manager (who is involved in purchasing and other financial processes) and IT Manager unnecessarily shared access to the shared user account, which had administrative permissions. The Operations Manager told us that she and the assistant operations manager rarely used the shared account.

The Operations Manager told us they had access to the account to serve as the IT Manager's backup during his absence, if needed (the IT Manager was the financial software administrator). However, officials could have ensured that the IT Manager assigned another IT staff member to serve as his backup. When users share accounts, accountability is diminished and financial software activity may not be able to be traced back to a single user.

We examined the financial software and found that School officials did not ensure that access controls were adequate or establish compensating controls for the software control deficiencies. It also did not have necessary controls to maintain data integrity and deter inappropriate activity. The software allowed users to make changes to and delete transaction data – such as voiding transactions and deleting and adjusting data, including vendor names and disbursement amounts – without approval.

As a result, the School has an increased risk that unauthorized changes to the accounting records, software security settings and user authorization privileges could occur and go undetected. The risks associated with these inadequately controlled financial software permissions are increased because the Operations Manager signs School disbursement checks (under \$5,000) using the Director's

signature stamp without adequate oversight by the Director or another individual. When combined, these inadequate controls increase the risk of inappropriate School disbursements occurring and not being detected and corrected.

School officials did not establish adequate compensating controls for the software's deficiencies. For example, although audit trail and activity reports (such as a report of voided and deleted transactions) were available in the financial software, no one generated and reviewed them to determine who accessed the software and what activities they performed.

In addition, although officials performed an independent review of the School's bank statements, they did not review canceled check images because the images were not included with the bank statements. Therefore, no one reviewed the actual checks to determine whether they were written to the same vendors as recorded in the financial software.

We reviewed the sequence of recorded check numbers, the software's voided and deleted transactions report for entries that reduced cash and a sample of 55 check disbursements totaling \$556,627.³ We did not identify any questionable activity and found that all 55 check disbursements were for appropriate School purposes.

While we did not identify any questionable activity, allowing individuals the ability to alter, add and delete financial software data without oversight and approval increases the School's risk that inappropriate transactions could occur and remain undetected. For example, a user could conceal a theft by issuing an unauthorized check and then deleting the check or changing the vendor name in the financial software to conceal the inappropriate transaction. Because School officials did not review audit trail reports, including the voided and deleted transaction reports, School officials' ability to detect and properly address inappropriate activity was diminished.

Also, when School officials do not require each user to have and use a unique username and password and do not limit user permissions to only those needed for job duties, the School has an increased risk that unauthorized or inappropriate activity could occur within the financial software. Furthermore, when users share an account, accountability is diminished and questionable activity within the financial software may be difficult to trace to a specific user.

³ Refer to Appendix B for further information on our sample selection.

How Does a Written Agreement With the IT Service Provider Help Ensure Network and Financial Software Access Controls Are Adequate?

To help adequately control a school's network and financial software access, and avoid potential misunderstandings, school officials should have a written agreement with the school's IT service provider. This agreement should establish the school's needs, clearly identify the IT service provider's roles and responsibilities and set the school's service expectations. The agreement also should include pricing, billing, payment terms and provisions for confidentiality to protect PPSI.

Furthermore, the agreement should be as specific as possible to establish comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. Agreements that are unwritten or lack these details can lead to indecision, disagreements or additional unanticipated costs. Officials should also periodically monitor the agreement to ensure compliance.

The School Did Not Have an Adequate Written Agreement with the School's IT Service Provider

School officials engaged an IT service provider to manage the School's IT operations, including support and services for network and financial software access controls. School officials had a written agreement with the IT service provider that contained provisions for pricing, billing, payment terms and protecting PPSI.

However, the agreement did not provide detailed information for the services to be provided, explain School and IT service provider responsibilities, or include comprehensive measurable performance targets. For example, the School's agreed upon compensation for all IT support and services for the 2021-22 school year was \$90,922. But the agreement did not break down costs in detail to indicate the specific cost for each service, including those services directly related to network and financial software access controls.

Although the Operations Manager was responsible for overseeing the IT service provider, officials did not have procedures to monitor and review the work performed by the IT service provider. Therefore, officials could not ensure that the School's network and financial software data was adequately safeguarded.

Without an adequate written agreement and monitoring procedures, the School and IT service provider did not have stated responsibilities and procedures for network and financial software access controls. This can contribute to confusion over responsibilities for the various aspects of the School's network and financial

software access control management, which could put the School's resources and data at greater risk for unauthorized access, misuse or loss.

Why Should School Officials Provide IT Security Awareness Training?

To help minimize the risk of unauthorized access to the network and financial software, and misuse or loss of data and PPSI, officials should provide periodic IT security awareness training that explains the risks inherent in – and proper user behavior needed when – accessing and using the network and financial software. In addition, the training should communicate related policies and procedures to all network and financial software users, including contractors.

The training could center on emerging cyberattack trends, such as information theft, social engineering attacks (methods used to deceive users into revealing confidential or sensitive information) and computer viruses and other types of malicious software. It could also explain how these trends and malicious software could result in the School's network, financial software and data being compromised, or users being denied access to them.

In addition, the training should cover key security concepts, such as the dangers of email, Internet browsing and downloading files and programs from the Internet; requirements related to protecting PPSI on the network or in the financial software; and how to respond if an information security or data breach is detected.

School Officials Did Not Provide IT Security Awareness Training

School officials did not ensure that network and financial software users received periodic IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data and IT assets when accessing the network and financial software. The Director told us that they did not previously consider implementing IT security awareness training. However, this is a basic and fundamental security practice of which School officials or the School's IT service provider should have been aware.

Without periodic comprehensive IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of situations that could compromise the School's network and financial software. As a result, data and PPSI are at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

The Board should:

1. Develop and adopt adequate written policies related to network and financial software access, including password, remote access and breach notification policies, and policies related to managing user accounts and reviewing network and financial software audit trails.
2. Develop and adopt a written IT contingency plan.
3. Ensure that the School's written agreement with its IT service provider includes the School's specific needs and expectations for IT services, roles and responsibilities of all parties, and comprehensive measurable performance targets.

The Operations Manager should ensure the IT service provider:

4. Disables unneeded network and financial software accounts or removes unneeded user permissions in a timely manner as directed by School officials.
5. Regularly generates user accounts and permissions reports for the network and financial software and submits the reports to School officials for review.
6. Eliminates shared user accounts for the network and financial software, or implements procedures to compensate for the inadequate user accountability of the shared accounts.

The Director should:

7. Sign checks or provide adequate oversight of her signature stamp.

School officials should:

8. Designate a backup financial software administrator who is not involved in the School's financial operations.
9. Consider using alternative financial software or implement compensating controls for the software's deficiencies, such as an independent review of audit trail and change reports, canceled check images and check number sequences.
10. Provide periodic IT security awareness training to all network and financial software users.

Appendix A: Response From School Officials



January 30, 2022

Edward V. Grant, Jr.
Division of Local Government
and School Accountability
Office of the New York State Comptroller
110 State Street
Albany, NY 12236

Dear Mr. Grant,

We have received the draft audit report and have met with your team to review the findings and recommendations. We are in agreement with all recommendations.

The Board and School Administration will work to develop a comprehensive corrective action plan to address the findings and recommendations and will continue to improve our operations.

Sincerely,

Sara Castner
School Director

Discovery Charter School * 133 Hoover Drive Rochester NY 14626 * (585) 342-4032

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in in Section 2854 of the New York State Education Law, as amended by Chapter 56 of the Laws of 2014. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the School's IT and check disbursement policies and procedures and interviewed School officials and IT staff to gain an understanding of IT operations and controls, specifically those related to network and financial software access.
- We examined network user accounts and permissions using a computerized audit script, which we ran on March 30, 2022. We reviewed network user accounts and compared them to current employee lists to identify unused and possibly unneeded network user accounts and permissions. We discussed possibly unneeded network user accounts and permissions with School officials.
- We examined financial software user accounts and permissions as of March 10, 2022. We reviewed permissions for all three financial software user accounts to determine whether access was necessary and appropriate based on job duties and responsibilities.
- We reviewed recorded check number sequences and followed up on gaps in the numbering sequence, such as voids, because the financial software allowed changes and deletions to data.
- We assessed the adequacy of the School's written agreement with its IT service provider.
- We used our professional judgment to select 35 check disbursements (including all disbursements to business office staff and select disbursements for other School employees, the financial consultant and various vendors) and used a random number generator to select 20 check disbursements (55 disbursements) totaling \$556,627. Our sample represented 10 percent of the 534 check disbursements totaling \$3.3 million from July 1, 2020 through February 10, 2022. We chose this time period because it was the beginning of our audit period through the day after we held our entrance conference with School officials. We reviewed the supporting documentation (such as purchase order, purchase request forms and invoices) for the 55 disbursements to determine whether the disbursements were for a valid School purpose. We also compared the recorded disbursements to canceled check images.
- We reviewed all voided and deleted transactions (listed on a report generated from the financial software) that reduced cash during the period July 1, 2020 through May 5, 2022. We chose this time period because it was the beginning of our audit period through the date when we requested the

report. We compared the deleted transactions to general ledger activity to determine whether the deletions were reasonable (e.g., reversing duplicate entries). We reviewed supporting documentation for voided transactions to determine the reasons for the voids. We also reviewed bank statements to determine whether any voided or deleted checks cleared the bank.

Our audit also examined the adequacy of certain network and financial software access controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to School officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. We encourage the Board to prepare a plan of action that addresses the recommendations in this report and forward the plan to our office within 90 days. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the School's website for public review.

Appendix C: Resources and Services

Regional Office Directory

www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas

www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems

www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management

www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans

www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders

www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller

www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers

www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics

www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236
Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov
www.osc.state.ny.us/local-government
Local Government and School Accountability Help Line: (866) 321-8503

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits
The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608
Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov
Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

osc.state.ny.us

