

DOCKET NO.: UWY-CV-25-6084708-S	:	SUPERIOR COURT
	:	
OLIVIA LEARY, NATALIE HUDSON,	:	COMPLEX LITIGATION DOCKET
HANNAH KENT, LILY SCOFIELD,	:	
JORIE MCGURK, SAMANTHA	:	
THOMPSON, HAZEL GARRITY,	:	
DYMOND JOHNSON,	:	
JANE DOE #1, JANE DOE #2, JANE DOE #3,	:	
JANE DOE #4, JANE DOE #5, LIA FADIMAN,	:	
GABRIELLA POTH, SUZANNA KINGSLEY	:	
TUCKER, MELANIYA MARKARYAN,	:	
individually and on behalf	:	
of all others similarly situated,	:	
	:	AT WATERBURY
	:	
Plaintiffs,	:	
V.	:	
	:	
KENT SCHOOL CORPORATION, d/b/a	:	
KENT SCHOOL	:	
	:	
Defendant	:	APRIL 15, 2026

CONSOLIDATED AND AMENDED CLASS ACTION COMPLAINT

1. Plaintiffs Olivia Leary, Natalie Hudson, Hannah Kent, Lily Scofield, Jorie McGurk, Samantha Thompson, Hazel Garrity, Dymond Johnson, Jane Doe #1, Jane Doe #2, Jane Doe #3, Jane Doe #4, Jane Doe #5, Lia Fadiman, Gabriella Poth, Suzanna Kingsley Tucker, and Melaniya Markaryan (“Plaintiffs”), former students at Kent School in Kent, Connecticut, bring this action individually and on behalf of all others similarly situated whose computers were accessed and whose computer contents, including highly private and personal photographs (including photographs of a sexual and intimate nature), videos, and communications, were transferred, viewed, retained, and utilized, without their knowledge or consent, by Daniel Clery (“Clery”), a senior level administrator of Defendant Kent School Corporation (“Kent School”). Kent School employed Clery for 23 years, elevating him to the position of Network and Systems Administrator,

a job that provided him with high-level access to Kent School's servers and networks, and authorized and enabled him to access student computers and other personal devices on a regular basis. Throughout the Class Period, Kent School failed to implement reasonable security measures for its IT environment. Even after being put on notice by a female staff member in 2022 that Clery had improperly accessed and viewed her personal photos, Kent School failed to investigate or otherwise take action to safeguard and secure the personal photos and information of its students or otherwise protect their safety and well-being, intentionally choosing instead to turn a blind eye to Clery's activities. Eight months later, when Clery targeted the same staff member again and she again reported him, Kent School belatedly took action to investigate. Kent School discovered that Clery had been accessing and transferring the computer contents of at least 70 current and former students (including at least 68 female students) and 11 current and former female staff members over a period of years. Clery was terminated by Kent School in 2023 and is currently the subject of an ongoing criminal prosecution in which he has pled guilty to two felony counts of computer crimes committed for a sexual purpose. The allegations in this Complaint are based upon the investigation of plaintiffs' counsel; publicly available information, including information regarding the active criminal prosecution of Daniel Clery; the post-incident investigation done by Kent School and its outside IT consultant; information and belief; and personal knowledge.

2. Plaintiffs, individually and on behalf of a Class of Kent School's current and former students who had their computer contents accessed, viewed, transferred, retained, and utilized by Clery with Kent School's authority and facilitation, bring this class action against Defendant Kent School for damages as a result of Kent School's negligence; recklessness; and violations of the Connecticut Unfair Trade Practices Act, Gen. Stat. § 42-110a *et seq* ("CUTPA").

3. In addition to the class allegations, plaintiffs in their individual capacities bring this action against Defendant Kent School for damages as a result of Kent School's invasion of their privacy interests; computer privacy violations; and negligent infliction of emotional distress.

4. As used in this Complaint, "sensitive personal information" includes images, intimate photographs and videos, credit card information, social security numbers, phone numbers, addresses, birthdates, financial information, educational history, and medical information.

5. As used in this Complaint, "the Kent School network" includes the defendant's network infrastructure, IT infrastructure, IT framework, software, hardware, services, applications, operating systems, computing platforms, networking and communications, data storage and management.

6. As used in this Complaint "personal electronic devices" or "PEDs" includes cell phones, tablets, laptops or other computer devices.

PARTIES

PLAINTIFFS

7. Plaintiff Olivia Leary is a 23-year-old former student of Kent School and a resident of Goshen, Connecticut. From September of 2017 to September 2020, she was a minor student at Kent School. She remained a student after turning 18 and graduated in May 2021. Ms. Leary enrolled as a boarding student for one year and as a day student for three years.

8. Plaintiff Natalie Hudson is a 21-year-old former student of Kent School and a resident of Sharon, Connecticut. She was a minor student at Kent School from September 2018-May 2022. Ms. Hudson enrolled as a boarding student for one year and as a day student for three years.

9. Plaintiff Hannah Kent is a 22-year-old former student of Kent School and a resident of Halifax, Nova Scotia. She is currently a college student in New York State. She was a minor boarding student at Kent School from September 2017 to May 2021.

10. Plaintiff Lily Scofield is a 21-year-old former student of Kent School and a resident of Kent, Connecticut. She was a minor student at Kent School from September 2018 to May 2022. Ms. Scofield was enrolled as a boarding student for one year and as a day student for three years.

11. Plaintiff Jorie McGurk is a 21-year-old former student of Kent School and a resident of Kent, Connecticut. She was a minor day student at Kent School from September 2019 to January 2023. She remained a student after turning 18, and graduated in May 2023.

12. Plaintiff Samantha Thompson is a 24-year-old former student of Kent School and is a current resident of Philadelphia, PA. She was a minor day student at Kent School from September 2015 to May 2019.

13. Plaintiff Hazel Garrity is a 27-year-old former student of Kent School and is a current resident of Atlanta, GA. She was a student at Kent School from September 2013 to May 2017, during virtually all of which time she was a minor. For her first three years at Kent School, Ms. Garrity was a day student; during her fourth year at Kent School, Ms. Garrity boarded at Kent School.

14. Plaintiff Dymond Johnson is a resident of Florida, and a student at a college in Connecticut. From August of 2020 to June of 2024, she was a minor student at Kent School. Her parents entered into an agreement with Kent School whereby she was admitted and enrolled as a boarding student in exchange for monetary payment.

15. Plaintiff Jane Doe #1 is a resident of New Canaan, Connecticut. From September 2017 to May 2021, she was a minor student at Kent School. Jane Doe #1's parents entered into an

agreement with Kent School whereby Jane Doe #1 was admitted and enrolled as a boarding student in exchange for monetary payment.

16. Plaintiff Jane Doe #2 is a resident of Wilton, Connecticut. From September of 2017 to May of 2021, she was a minor student at Kent School. Jane Doe #2's parents entered into an agreement with Kent School whereby Jane Doe #2 was admitted and enrolled as a boarding student in exchange for monetary payment.

17. Plaintiff Jane Doe #3 is a resident of New York, NY. From September 2018 to May 2022, she was a minor student at Kent School. Jane Doe #3's parents entered into an agreement with Kent School whereby Jane Doe #3 was admitted and enrolled as a boarding student in exchange for monetary payment.

18. Plaintiff Jane Doe #4 is a resident of Hong Kong. From September 2018 to May 2022, she was a minor student at Kent School. Jane Doe #4's parents entered into an agreement with Kent School whereby Jane Doe #4 was admitted and enrolled as a boarding student in exchange for monetary payment.

19. Plaintiff Jane Doe #5 is a resident of Woodbridge, Connecticut. From September 2020 to March 2022, she was a minor student at Kent School. She remained a student after turning 18, and graduated in May 2022. Her parents entered into an agreement with Kent School whereby she was admitted and enrolled as a boarding student in exchange for monetary payment.

20. Plaintiff Lia Fadiman is a resident of Shelton, Connecticut. From September 2017 to May 2021, she was a minor student at Kent School. Lia's parents entered into an agreement with Kent School whereby Lia was admitted and enrolled as a boarding student in exchange for monetary payment.

21. Plaintiff Gabriella Poth is a resident of Ridgefield, Connecticut. From September 2017 to June 2019, she was a minor student at Kent School. Gabriella's parents entered into an agreement with Kent School whereby Gabriella was admitted and enrolled as a boarding student in exchange for monetary payment.

22. Plaintiff Suzanna Kingsley Tucker is a resident of Georgia. From September 2018 to December 2020, she was a minor student at Kent School. She remained a student after turning 18 and graduated in May 2021. Her parents entered into an agreement with Kent School whereby she was admitted and enrolled as a boarding student in exchange for monetary payment.

23. Plaintiff Melaniya Markaryan is a resident of New York. From September 2018 to May 2021, she was a minor student at Kent School. She remained a student after turning 18 and graduated in May 2021. Her parents entered into an agreement with Kent School whereby she was admitted and enrolled as a boarding student in exchange for monetary payment.

DEFENDANT

24. Defendant Kent School Corporation is a corporation formed pursuant to the laws of the State of Connecticut, and at all times relevant to this Complaint owned and operated Kent School, a private boarding school located at One Macedonia Road, Kent, Connecticut.

SUBSTANTIVE ALLEGATIONS

25. Kent School is a co-educational, independent college preparatory boarding school for grades 9-12 located on 1,200 acres in Kent, CT. It serves approximately 520 students, approximately 90+ percent of whom are boarding students and the remainder of whom are day students. According to its website, Kent School “foster[s] deep relationships that prepare our students to contribute to the common good in the world beyond Kent,” and its “[s]tudents and faculty live together on campus and work purposefully to establish a culture of compassion,

inclusivity, respect, and safety in and out of the dorms.” With respect to the importance of residential life to the educational experience, Kent School states that “[r]esidential life at Kent creates a living atmosphere in which the campus becomes your home away from home and the community becomes family.” Kent School’s website emphasizes that “[t]he “Kent experience is only possible when we prioritize the health, safety, and positive growth of students.”

26. Clery was hired by Kent School in August 2000 to work in its IT department as a PC Support Specialist. In July 2012, he was promoted to Network and System Administrator. In this position, he held the highest level of network access. He held this position for over 10 years until his termination by Kent School on February 27, 2023.

27. As Network and Systems Administrator, Clery was responsible for implementing and maintaining the school’s servers and its networking capabilities. As part of his job, Clery routinely had access to student and staff laptops and routinely interacted with students.

28. At all relevant times, Kent School knew, or had reason to know, that Daniel Clery, via his position at Kent School, had unrestricted access to the personal electronic devices (“PEDs”) of minor students, including to those of the plaintiffs and class members.

29. At all relevant times, Kent School knew, or had reason to know, that Daniel Clery, via his position at Kent School, had unrestricted access to the Kent School network.

30. At all relevant times, Kent School authorized and required Daniel Clery to offer students, including the plaintiffs, services relating to their PEDs and the Kent School network.

31. At all relevant times, Kent School knew, or had reason to know, that Daniel Clery's position with Kent School enabled him to take possession of the PEDs of minor students, including the plaintiffs.

32. At all relevant times, Kent School knew, or had reason to know, that Daniel Clery's position with Kent School enabled him to access sensitive personal information of minor students, including plaintiffs, stored on the Kent School network.

33. Without the knowledge or consent of the plaintiffs or their parents, and while acting within the scope and course of his agency and/or employment with the defendant, Daniel Clery cyberstalked, surveilled, and sexually exploited minor students, including the plaintiffs, through voyeuristic actions infiltrating the plaintiffs' PEDs.

34. At all times relevant to plaintiffs' and the Class's claims herein, Clery was acting as an employee, servant, agent, apparent agent and/or authorized representative of Kent School within the scope of his employment.

35. At all times relevant to plaintiffs' and the Class's claims of liability, Kent School was responsible for supervising, overseeing, and monitoring Clery's actions in his capacity as Kent School's Network and Systems Administrator, including but not limited to ensuring that Clery did not intentionally injure plaintiffs, any members of the Class, or any members of the Kent School community.

36. By authorizing and allowing Clery to function as a Network and Systems Administrator and by encouraging private interactions between Clery and Kent School students and other members of the Kent School community, Kent School represented to plaintiffs and to members of the Class that Clery was fit, qualified, and competent to serve as Network and Systems Administrator and to provide plaintiffs and members of the Class with technological services and guidance.

I. KENT SCHOOL IS PUT ON NOTICE THAT CLERY WAS USING HIS AUTHORIZED ACCESS AS A NETWORK ADMINISTRATOR TO ACCESS, MISUSE AND STEAL THE PERSONAL INFORMATION OF KENT SCHOOL COMMUNITY MEMBERS.

37. In the spring or summer of 2022, a female Kent School employee (“KC”) reported to Clery that she was having Wi-Fi trouble with the laptop that she had been issued by Kent School. Clery, in his capacity as Network and Systems Administrator, came to KC’s office to troubleshoot. He told KC that “this will take a while,” and suggested that she leave the office while he was working on her laptop. KC left for a few minutes; and when she returned to her office, she could see on her Kent laptop monitor that Clery was scrolling through her personal photos. KC recognized that the sequence of photos that Clery was viewing contained, in addition to family photos, intimate photographs of a sexual nature that were intended for her husband’s eyes only. When Clery became aware that KC had reentered the room, he quickly closed the screen.

38. Extremely distressed by this, KC notified Christina Memoli, the Kent School Director of Studies and KC’s direct supervisor, that she had just caught Clery looking at her personal photographs. In her authority as a school official and KC’s direct supervisor, Memoli had a duty to report the serious allegations made by KC about a member of Kent School staff who was reported to be engaging in such egregious conduct.

39. Soon thereafter, Robert Duncan, a Technical Support Specialist in Kent School’s IT Department, happened to come to KC’s office on an unrelated matter. KC also reported to Duncan that she had caught Clery scrolling through her personal photos. Duncan responded by acknowledging that “[Clery is] a weird dude.” In his authority as a member of the IT Department, Duncan had a duty to report the serious allegations made by KC about a member of his department who was reported to be engaging in such egregious conduct.

40. No action was taken by KC's supervisor Christina Memoli, despite her responsibility to report allegations that had the potential to (and did in fact) put the entire Kent School community at risk. Similarly, no action was taken by Robert Duncan or anyone else in the IT Department to safeguard the community. Indeed, nobody at Kent School investigated or took any action after it was alerted or should have been alerted to Clery's actions in the spring or summer of 2022. Clery continued his employment at Kent School and continued to be given the highest level of access to Kent School's network and systems, including access to student and employee laptops.

41. On February 21, 2023, approximately eight months after KC caught Clery viewing her personal photographs on her computer, KC was approached by Clery, who advised her that he was working on a Kent School IT Department project involving a security audit, and that he needed to access her Kent School-issued laptop. KC was suspicious of Clery's request to access her computer and inquired whether he was performing a similar audit on other people's computers, and whether she was the "first stop." Clery assured KC that he was performing the same check on other computers but indicated that she was the first stop. KC did not leave Clery alone with her computer.

42. After Clery completed his work and left KC's office, she received an email to her Kent School email account (which was the recovery email for her personal email account) notifying her that a software product called RClone had been granted permission to access her personal Google account. At no time did KC authorize Clery or Kent School to access her personal Google account.

43. When KC received the email to her Kent School email account notifying her that the RClone software had been granted permission to access her personal Google account, she

notified Michael Siepmann, the head of Kent School's IT Department, and asked him what RClone was. Siepmann was unaware of the use or existence of RClone software in Kent School's IT environment. KC also told Siepmann about having caught Clery scrolling through her personal photos eight months earlier. Siepmann replied, "That's weird," and told KC that he would talk to Clery.

44. RClone is an open source, command line computer program utilized to manage or migrate content on cloud storage. RClone allows the user to sync and transfer files across electronic storage devices.

45. Siepmann contacted Clery who said he used RClone to copy the school's antivirus logs and must have "accidentally" configured RClone to access KC's Google account. This explanation was patently fallacious and should have been understood as false by Siepmann. Upon information and belief, Siepmann then instructed Clery to return to KC's computer to rectify his "mistake."

46. Later that same day, when KC returned from lunch, Clery was pacing outside her office waiting for her, sweating, clearly agitated, and with his fly unzipped. He told her that he needed to access her computer again. This time, KC stood next to Clery as he worked on her computer. Clery's personal smartphone, an Android with a large display screen, was lying on KC's desk. KC noticed that Clery's phone lit up, and that her personal photos from a foreign vacation she had taken with one of her children three years previously were clearly visible in a gallery view on Clery's cell phone. Among the visible photos was a private nude photograph of herself that she had sent to her husband. KC demanded of Clery, "Are those my photos on your phone??" Clery responded, "No, um, no," and frantically grabbed his phone to try to close the app. KC asked Clery why her personal photos were on his cell phone and Clery replied, "I don't know. I'm sorry."

47. Feeling nauseous at the thought of Clery viewing her personal photos, KC went directly to the Kent IT Department and reported the incident to Siepmann and to the Kent School Head of Human Resources, Isabelle Benjamin, who was present in Siepmann's office. KC specifically told Siepmann and Benjamin that she had seen her personal photos on Clery's phone.

48. Siepmann and Benjamin told KC that they would speak to Clery.

49. As a result of this incident, Kent School belatedly initiated an internal investigation of Clery's conduct. During the course of the investigation, Clery admitted that he intentionally copied the access token to KC's Google Photos account to a Linux server called mc.kent-school.edu, which started syncing KC's photos to his cell phone.

50. Shortly after KC reported the incident to him, Siepmann asked for access to KC's computer to see how RClone was configured.

51. Kent School terminated Clery's employment on February 27, 2023, approximately eight months after KC first reported Clery's disturbing behavior and six days after she had reported Clery's actions to Michael Siepmann, the head of Kent School's IT Department, and to Isabelle Benjamin, the Kent School Head of Human Resources.

52. Firmly believing that she was not the only victim, KC repeatedly questioned the Kent School administration, including Jeff Cataldo, the Associate Head, Chief Financial Officer and Chief Operating Officer of Kent School, Siepmann, and Benjamin whether a crime had been committed, whether the personal photos and data of others, as well as her own, had been similarly accessed and breached, and whether the police should be notified.

53. On March 1, 2023, KC emailed Siepmann, Benjamin and Cataldo as follows:

I still feel unsettled that Dan [Clery] left Kent with my personal drive/information, possibly still on his phone. Wouldn't it be appropriate to report this breach of privacy as a crime?... I fear I may not be the first or last

victim of his misuse of power, and it isn't very comforting to think about him doing something like this at another school...

54. Dismissing KC's concerns, Cataldo emailed KC on March 2, 2023 that, since Clery's employment had been terminated, Kent School did not feel obligated to report Clery's actions to the police, that he was unsure whether a crime had been committed, and that he did not know whether Clery still had access to her personal information:

Dan Clery no longer has access to Kent resources that would provide access to any of your Kent School based technology... I cannot comment on whether Dan has left Kent School with information that is personal to you... Our review focused on whether Dan's behavior was unprofessional and inappropriate and focused on whether or not we lost confidence in Dan as a technology professional. We did not take actions to determine the status of data he may or may not have... Should you remain concerned that Dan still has personal information that belongs to you and/or you feel more needs to be done to manage this matter, you should feel free to report this incident to the police...I cannot comment on whether Dan's actions were criminal, I do not know. **After careful review I do not believe Kent School has an obligation to report this matter to the police.**

(Emphasis added).

55. Cataldo told KC that there was nothing Kent School had done wrong or could have done to prevent Clery's actions, since Clery had the highest possible security clearance and was, according to Cataldo, using software to which he had access as a routine part of his job. This was patently false. Kent School has subsequently implemented security protocols that would have prevented this very situation from occurring.

56. Kent School subsequently hired an information and cybersecurity firm called Vancord to conduct limited examinations of Clery's work computers and of the Kent School servers. As Siepmann described it to KC in a March 16, 2023 email, "[w]e are having a third party conduct a **small investigation** into the event that occurred. **This is an effort to verify that this was an isolated incident** and to gain further clarification on the technological aspect of this."

(Emphasis added). What Vancord discovered, however, was anything but “an isolated incident.” As part of this investigation, KC was asked to provide her computer so that Vancord could conduct a forensic analysis. KC complied with this request.

II. THE VANCORD INVESTIGATION FOUND WIDESPREAD EVIDENCE OF CLERY’S REPEATED AND EGREGIOUS CONDUCT INVOLVING AT LEAST 70 STUDENT VICTIMS OVER A PERIOD OF YEARS.

57. The Vancord investigation, which began on March 13, 2023, located logs showing that Clery had accessed and copied personal files, including images and video files, from the personal computers of approximately 81 Kent community members, including 70 current and former Kent School students, and 11 current and former employees.

58. Of Clery’s 81 victims, 79 were female. One of the two male victims was, at the time his information was misappropriated by Clery, the boyfriend of plaintiff Natalie Hudson.

59. The photographs were copied to accounts belonging to Clery on Kent School servers. Evidence was also found that Clery viewed the photos on Kent School servers. The Vancord investigator also located photographs of female Kent School students in the Recycle Bin of Clery’s work-issued laptop.

60. The Vancord investigation revealed that a software management system which Kent School deployed to support the school community was used by Clery specifically to target female students and to find and upload photos saved on their personal computers. Photos were processed on Kent School servers and were most likely stored in a cloud location. This activity dated back to at least the 2016-2017 school year and continued through February 2023.

61. The Vancord investigation also revealed that Clery used a Kent School software management system to configure “back door” remote access on his victims’ personal computer systems and to access these systems over Kent School’s network. The investigation found that

Clery added a local account to student computers during Kent School's onboarding process at the time the students matriculated, and that this was one method that he used to "backdoor" into student accounts. Clery was found to have frequently probed Kent School's network to discover online systems and logged into them.

62. The Vancord investigation further discovered that Clery had accessed numerous Kent School student accounts in Google by using his highly privileged Kent School IT administrator access. This included resetting passwords and generating "backup codes" to defeat multi-factor authentication when needed. Vancord was able to identify activities undertaken by Clery while using his Kent School account access that included viewing emails, taking photo or movie files, and in some cases creating access tokens to Google Photo Library.

63. The Vancord investigation also discovered evidence to support password hacking by Clery. Tools and techniques for recovering passwords from their encrypted forms were discovered. Review of Clery's web browsing history supported the finding that Clery was using his access to Kent School's IT system to gain access to the personal accounts of Kent School students and further showed signs of his interest in software piracy/cracking and pornography.

64. Vancord also discovered that by the time Kent School hired Vancord to conduct the investigation, Clery had deleted and/or otherwise secreted much of the evidence of his handling of his victims' photos; most evidence Vancord uncovered around this activity came from copies of files that were likely missed in Clery's deletion activities and command history that was also not cleared. Kent School student photos were discovered in several locations that Clery likely missed when attempting to delete evidence of his activities. Clery had also deleted data from his Kent School-issued laptop prior to being terminated from his employment at Kent School.

65. The Vancord investigation revealed that Clery employed several different methods to access his victims' personal computers.

66. First, Clery used his status as a Google administrator for Kent School to reset student passwords. Normally, access to student Google accounts would require knowledge of a user's password; in the event of a challenge, further multi-factor authentication would be required. A Google administrator is not normally able to access student or staff email in this manner. However, the Google administrator is able to reset passwords and generate back-up codes to bypass the multi-factor authentication, allowing the administrator to access Google accounts. Vancord's investigation showed that Clery used his high-level access, granted to him in his capacity as a Kent School Google administrator, to reset user passwords and generate backup codes, thus allowing him access to students' Google accounts and protected folders.

67. Once Clery gained access to Kent School student accounts, he used RClone to transfer student information, including photographs, videos and messages, to Clery's account on the Kent School's servers. Vancord found commands in the command history of the Kent School server that showed the use of RClone to transfer files from plaintiffs' and Class Members' accounts to Clery's account on the Kent School server.

68. Vancord also discovered evidence that Clery accessed the account of at least one student who had graduated from Kent School years earlier and was not at Kent School during the time the account was logged into; and that there were no "trouble tickets" or other student requests for IT help to indicate that this access was done at the student's request.

69. Second, the Vancord investigation also found that Clery was able to access students' personal computers through the use of another software management system called Munki. This system was deployed and used by Kent School to onboard new students and to connect them to

the school's wireless network. The Munki system would push necessary software to student computers, and the students' laptops would check in to the Kent School server automatically for software updates. Vancord located a script (a sequence of instructions that another program interprets and executes) with custom code that would search the student computers for photos and then transfer them to the Kent School server. The script was set to run each time a computer "pinged" back to the Munki system.

70. As a result of reviewing Clery's electronic work devices, Kent School servers, and server logs, Vancord was able to identify 81 individuals whose computers were accessed by Clery without their knowledge or permission and whose photos and videos had been transferred. These 81 individuals consisted of 58 former students, 12 current students, 7 current employees and 4 former employees.

71. On March 31, 2023, over a month after KC reported Clery for the second time to Kent School and after its initial refusal to report the matter to the police at KC's suggestion, Siepmann reported to the Connecticut State Police that Clery was believed to be remotely accessing the computers of current and former Kent School students and staff members.

III. THE INVESTIGATION BY THE CONNECTICUT STATE POLICE CONFIRMS WIDESPREAD EVIDENCE OF CLERY'S REPEATED AND EGREGIOUS CONDUCT INVOLVING AT LEAST 70 STUDENTS OVER A PERIOD OF YEARS.

72. A warrant was issued for Clery's arrest in June 2024, and Clery was charged with the crimes of Computer Crime in the First Degree (Unauthorized Access to a Computer System) in violation of Gen. Stats. § 53a-252 for accessing the computers of Kent School students and employees and Computer Crime in the First Degree (Misuse of Computer System Information) in violation of Gen. Stats. § 53a-252 for transferring Kent School students and employee image and video files from their computers to Clery's school-issued laptops and personal cell phone.

73. As part of its investigation into Clery's actions, the Connecticut State Police obtained search warrants for three personal laptop computers that had been turned into the school by students, including plaintiff Dymond Johnson, for the purpose of conducting a forensic analysis. In addition, the police examined the laptop of a fourth student, plaintiff Jorie McGurk, that had been provided to the police by Ms. McGurk's father. The State Police also obtained a search and seizure warrant to search Clery's house. The search resulted in the seizure of eight items, as well as of Clery's personal cell phone.

74. Forensic examination of Clery's seized computers uncovered the existence of 3,670 personal image files that potentially belong to or depict current and former Kent School students. The image files depicted text message/email screenshots as well as personal images of Kent School students. Some of the image files included images of female students naked, wearing lingerie/underwear, and wearing bikini bathing suits. Siepmann and Dale Reinhardt, the Kent School Dean of Students, were able to identify numerous Kent School students depicted in the photos copied and taken by Clery.

75. The forensic report confirmed that Clery had accessed Kent School student computers and executed commands that resulted in the copying and transfer of photographs, videos, and messages to Clery's account on Kent School's servers using RClone.

76. On the computer seized from the family room at Clery's residence, police found Google searches conducted between April 18-20, 2023 including:

- Privacy violation laws

- ECPA violation examples

- Warrant search Connecticut

- Snooping on someone's computer crime

- Teacher charged with looking at students photos

- Getting hired with black mark

Sued for invasion of privacy
Snooping compulsion
Snooping compulsion at work
Voyeurism crime
Mandatory reporting and nudity
Teacher creeping on photos

77. On March 16, 2026, Clery pled guilty to two felony counts of computer crimes committed for a sexual purpose. Pursuant to the plea, Clery is expected to receive a ten-year suspended sentence with five years of probation, which will include sex offender conditions of probation such as limited access to computers, and he will remain on the sex offender registry for ten years. Clery is expected to be sentenced on or about June 29, 2026.

IV. PLAINTIFFS AND THE CLASS HAD THEIR PERSONAL INFORMATION, INCLUDING HIGHLY SENSITIVE AND SEXUALLY INTIMATE PHOTOGRAPHS AND VIDEOS, ACCESSED, STOLEN, AND MISUSED BY CLERY, ACTING WITH KENT SCHOOL'S AUTHORITY AND FACILITATION.

78. Plaintiffs and all Class members were required to permit Kent School software to be installed on their personal laptop computers at the time they matriculated at Kent School in order to link their computers to the Kent network.

79. On April 18, 2023, the very day Clery was conducting the aforementioned Google searches, Kent School contacted the named plaintiffs and 65 other individuals to advise them that Clery had used his Kent School network authorization to obtain access to their private and personal photos, videos, and emails stored on their laptops from at least June 2019 through February 2023. In fact, Kent School either knew at the time or learned by the next day that Clery's activities dated "as far back as the school year 2016/17" meaning that he had access to, and the ability to steal and

otherwise misuse, the private and personal photos, videos, and emails of many hundreds of former Kent School students.

80. As required by Kent School, plaintiff Olivia Leary permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

81. In addition, Ms. Leary left her personal laptop computer with Clery for approximately a half-day on at least two occasions during her first and second years at Kent School in order for Clery to fix Wi-Fi, printer, and other computer issues that she was experiencing.

82. Ms. Leary's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

83. Ms. Leary was a minor under the age of 18 for her first three years at the Kent School, during at least part of which time Clery was accessing her computer.

84. As required by Kent School, plaintiff Natalie Hudson permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent School in order to link her computer to the Kent School network.

85. In addition, Ms. Hudson left her personal laptop computer with Clery for several hours on at least one occasion during her first or second year at Kent School in order for him to fix a Wi-Fi issue that she was experiencing.

86. Ms. Hudson's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

87. Ms. Hudson was dating one of the two male victims of Clery's computer misconduct at the time of the incident. Upon information and belief, Clery targeted the male victim

in order to gain greater access to highly private and sensitive pictures and/or videos of Ms. Hudson. Ms. Hudson was a minor under the age of 18 the entire time she was a student at the Kent School.

88. As required by Kent School, plaintiff Hannah Kent permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent School in order to link her computer to the Kent School network.

89. In addition, Ms. Kent left her personal laptop with Clery in the Kent School Tech Office on three separate occasions in order for Clery to fix Wi-Fi, printer, and other computer issues she was experiencing.

90. Ms. Kent also left her laptop in the Kent School Tech Office with Clery and two other employees who were also present in the office on two or three additional occasions in order for them to fix computer issues she was experiencing.

91. Ms. Kent also dropped off her cell phone for at least one hour at the Kent School Tech Office with Clery and another Kent employee in order for them to fix a Wi-Fi issue.

92. Ms. Kent, who played on the Kent School Girls' Lacrosse Team, also gave Clery her cell phone and/or laptop and/or emailed him one or more photos of female Kent School students playing lacrosse in order for him to blow the photos up into posters used by the Lacrosse Team.

93. Upon information and belief, the Kent School Tech Office, where Clery worked, was also the only location on campus where students could obtain color printouts of photos or other materials stored on their laptops or cell phones. Ms. Kent went there to obtain color printouts on multiple occasions and made her computer or cell phone available to Clery and other Kent School Tech Office employees in the process of doing so.

94. Ms. Kent's computer and cell phone contained highly private and sensitive photographs and videos that were improperly accessed by Clery. Ms. Kent was a minor under the age of 18 the entire time she was a student at Kent School.

95. As required by Kent School, plaintiff Lily Scofield permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

96. During her freshman year when she was 13 years old, Ms. Scofield was downloading songs from YouTube onto her personal laptop when pop-up browsers displaying pornography appeared on her laptop screen. Shocked and horribly embarrassed by this, and believing that she had a computer virus, she brought her laptop to Clery at the Kent School IT department for him to help her in deleting the virus.

97. To the best of her recollection, Clery told Ms. Scofield that he was going to download "Manwarning software," which he described as an IT app that blocks all viruses, assuring her "This gets rid of everything." Ms. Scofield left her laptop with Clery for a full day in order for him to download the software he had described.

98. Ms. Scofield's laptop computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery. Ms. Scofield was a minor under the age of 18 the entire time she was a student at Kent School.

99. As required by Kent School, plaintiff Jorie McGurk permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

100. On one occasion during her junior or senior year, Ms. McGurk had trouble connecting to a printer and brought her laptop to the Kent IT Department in search of assistance.

As another male IT Department employee helped her, Clery sat right next to him, and clearly eyed Ms. McGurk.

101. Ms. McGurk was a minor under the age of 18 for most of her time at Kent School, during which time Clery was accessing her computer.

102. Ms. McGurk's computer contained private photographs and videos, including images of her minor cousins and/or friends in bathing suits at the beach and images of her during dance recitals wearing skin-tight dance leotards, that were improperly accessed by Clery.

103. After Clery's actions came to light and Ms. McGurk provided her compromised personal laptop to the Connecticut State Police as evidence of Clery's actions, Kent School offered Ms. McGurk a replacement MacBook Air laptop computer. No longer willing or able to trust Kent School or its IT Department in any way, Ms. McGurk insisted that she be provided with a brand-new laptop, to be delivered to her school mailbox in a sealed box, as she wanted no further interactions with the Kent IT Department; and she arranged to have it configured independently of the Kent IT Department, as she no longer trusted anyone at Kent to access her personal computer.

104. As required by Kent School, plaintiff Samantha Thompson permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

105. Ms. Thompson's laptop computer experienced operating issues in her freshman year and she brought her laptop to the Kent School IT department and gave it to Clery for repair. She recalls feeling very uncomfortable sitting in a dark room on that occasion with Clery and one other male IT Department employee as she explained what was wrong with her laptop. She recalls that Clery's pants sagged, exposing part of his buttocks, and that his belt was too loose. She was

given a loaner computer; and Clery retained possession of Ms. Thompson's laptop computer for a period of approximately three to six days.

106. On one occasion likely during her junior year, Ms. Thompson's cell phone stopped functioning properly. She handed it over to the Kent School IT department for repair for at least one full day.

107. Ms. Thompson recalls that Clery frequently lurked by the IT Department door and eyed her and said hello to her on multiple occasions when she passed by or when she saw him in other campus locations.

108. Ms. Thompson's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

109. Ms. Thompson was a minor under the age of 18 during the entire time she was a student at Kent School, during which time Clery was accessing her computer.

110. As required by Kent School, plaintiff Hazel Garrity permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

111. Ms. Garrity brought her laptop to the Kent School IT Department frequently during her years at Kent School where it was worked on by various members of the IT Department, including Michael Siepmann and Daniel Clery.

112. On one morning most likely during her junior year, Ms. Garrity, who was a minor at the time, brought her laptop into the Kent School IT Department for repair. Clery told her that "this is going to take a while," and suggested that she leave her laptop with him for several hours and return for it at the end of the school day. Ms. Garrity complied with Clery's instruction, returning to pick up her laptop at about 3:15 PM.

113. Ms. Garrity's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

114. In approximately April 2025, Ms. Garrity was contacted by the Connecticut State Police who asked her to identify herself in photos recovered from Clery's laptop or other PEDs as part of their investigation. She was shown approximately 15-20 photos, and was able to identify herself in all but one photo. The photos of herself that were recovered from Clery's possession, custody or control contained highly private and sensitive photographs taken while Ms. Garrity was a minor student at Kent School, as well as baby pictures of Ms. Garrity in her bath when she was approximately two years old.

115. As required by Kent School, plaintiff Dymond Johnson permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

116. During her time as a student at Kent School, Ms. Johnson stored sensitive personal information on her PEDs, including pictures and videos of herself, her friends, and her relatives, who were all minors when the photos were taken.

117. In addition, in 2022, Ms. Johnson visited the Kent IT Department on multiple occasions because she was having trouble with her laptop battery. She was required by Kent IT Department staff, including Clery, to leave her personal laptop computer, Apple ID, and password at the Kent ID Department on several occasions so they could purportedly fix the issue.

118. Ms. Johnson's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

119. Ms. Johnson was a minor under the age of 18 for her time at Kent School, during which time Clery was accessing her PEDs.

120. After Clery's actions came to light, Ms. Johnson provided her compromised personal laptop to the Connecticut State Police as evidence of Clery's actions, and Kent School offered Ms. Johnson a replacement MacBook Air laptop computer.

121. As required by Kent School, plaintiff Jane Doe #1 permitted Kent School software to be installed on her personal laptop computers at the time she matriculated at Kent in order to link her computer to the Kent School network.

122. During her time as a student at Kent School, Ms. Doe #1 stored sensitive personal information on her PEDs, including pictures and videos of herself, her friends, and her relatives, who were all minors when the photos were taken.

123. In addition, on multiple occasions during her time at Kent School, Ms. Doe #1 left her personal laptop computers with Clery in the Kent IT Department, always with her password written down in accordance with Clery's instruction. Clery kept each of these laptop computers, purportedly to fix them, for several days before giving them back to Ms. Doe #1.

124. Ms. Doe #1's computers contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

125. Ms. Doe #1 was a minor under the age of 18 for her time at Kent School, during which time Clery was accessing her PEDs.

126. As required by Kent School, plaintiff Jane Doe #2 permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

127. During her time as a student at Kent School, Ms. Doe #2 stored sensitive personal information on her PEDs, including pictures and videos of herself, her friends, and her relatives, who were all minors when the photos were taken.

128. In addition, during her time at Kent School, on several occasions, Ms. Doe #2 left her personal laptop computer with Clery in the Kent IT Department, always with her password written down in accordance with Clery's instruction. On these occasions, Clery kept the laptop computer, purportedly to fix it, for several hours to days before giving it back to Ms. Doe #2.

129. Ms. Doe #2's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

130. Ms. Doe #2 was a minor under the age of 18 for her time at Kent School, during which time Clery was accessing her PEDs.

131. As required by Kent School, plaintiff Jane Doe #3 permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

132. During her time as a student at Kent School, Ms. Doe #3 stored sensitive personal information on her PEDs, including pictures and videos of herself, her friends, and her relatives, who were all minors when the photos were taken.

133. In addition, during her time at Kent School, on at least two occasions, Ms. Doe #3 left her personal laptop computer with Clery in the Kent IT Department, with her password written down in accordance with Clery's instruction. On these occasions, Clery kept the laptop computer, purportedly to fix it, for several days before giving it back to Ms. Doe #3.

134. Ms. Doe #3's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

135. Ms. Doe #3 was a minor under the age of 18 for her time at Kent School, during which time Clery was accessing her PEDs.

136. As required by Kent School, plaintiff Jane Doe #4 permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

137. During her time as a student at Kent School, Ms. Doe #4 stored sensitive personal information on her PEDs, including pictures and videos of herself, her friends, and her relatives, who were all minors when the photos were taken.

138. In addition, during her time at Kent School, Ms. Doe #4 reached out to Clery via email for help connecting a lightbulb which had Bluetooth and Wi-Fi capabilities to the school network, so she could control its function. During this exchange, Clery used his position with the Kent IT Department to scare and manipulate Ms. Doe #4 into believing that there was suspicious activity coming from her iPhone. Clery convinced Ms. Doe #4 that she needed to bring her iPhone to Clery and provide her passcodes so that he could access it purportedly to fix the iPhone. Clery kept the iPhone, purportedly to fix it, for several hours before giving it back to Ms. Doe #4.

139. Ms. Doe #4's computer, which linked to her iPhone, and her iPhone, contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

140. Ms. Doe #4 was a minor under the age of 18 for her time at Kent School, during which time Clery was accessing her PEDs.

141. As required by Kent School, plaintiff Jane Doe #5 permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

142. During her time as a student at Kent School, Ms. Doe #5 stored sensitive personal information on her PEDs, including pictures and videos of herself, her friends, and her relatives, who were all minors when the photos were taken.

143. On at least one occasion, Ms. Doe #5 left her personal laptop computer with Clery in the Kent IT Department, with her password written down in accordance with Clery's instruction. Clery kept the laptop computer, purportedly to fix it, for several hours before giving it back to Ms. Doe #5.

144. Ms. Doe #5's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

145. Ms. Doe #5 was a minor under the age of 18 for the majority of her time at Kent School, during which time Clery was accessing her PEDs.

146. As required by Kent School, plaintiff Lia Fadiman permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

147. During her time as a student at Kent School, Ms. Fadiman stored sensitive personal information on her PEDs.

148. On at least two occasions, Ms. Fadiman left her personal laptop computer with Clery in the Kent IT Department, with her password written down in accordance with Clery's instruction. Clery kept the laptop computer, purportedly to fix it, for several hours before giving it back to Ms. Fadiman.

149. Ms. Fadiman's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

150. Ms. Fadiman was a minor under the age of 18 for the majority of her time at Kent School, during which time Clery was accessing her PEDs.

151. As required by Kent School, plaintiff Gabriella Poth permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

152. During her time as a student at Kent School, Ms. Poth stored sensitive personal information on her PEDs.

153. On several occasions, Ms. Poth left her personal laptop computer with Clery in the Kent IT Department, with her password written down in accordance with Clery's instruction. Clery kept the laptop computer, purportedly to fix it, for several hours before giving it back to Ms. Poth.

154. Ms. Poth's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

155. Ms. Poth was a minor under the age of 18 for the majority of her time at Kent School, during which time Clery was accessing her PEDs.

156. As required by Kent School, plaintiff Suzanna Kingsley Tucker permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

157. During her time as a student at Kent School, Ms. Tucker stored sensitive personal information on her PEDs.

158. In 2018, Ms. Tucker left her iPhone and laptop with Clery, with her passwords written down in accordance with Clery's instruction, so that he could download the software used to connect to the Kent School network. Clery kept the iPhone and laptop computer for several hours before giving them back to Ms. Tucker. Clery had installed software on her laptop that uploaded all of her photos from her camera roll into her Kent School Google Drive. On another occasion in 2020, Ms. Tucker's computer stopped charging, so she brought it to the Kent IT

Department. Again, Clery instructed Ms. Tucker to write down her password. Clery kept the laptop for a week before giving it back to Ms. Tucker.

159. Ms. Tucker's computer contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

160. Ms. Tucker was a minor under the age of 18 for the majority of her time at Kent School, during which time Clery was accessing her PEDs.

161. As required by Kent School, plaintiff Melaniya Markaryan permitted Kent School software to be installed on her personal laptop computer at the time she matriculated at Kent in order to link her computer to the Kent School network.

162. During her time as a student at Kent School, Ms. Markaryan stored sensitive personal information on her PEDs.

163. On at least three occasions, Ms. Markaryan left her personal laptop computer and iPhone with Clery in the Kent IT Department, with her password written down in accordance with Clery's instruction. Clery kept the iPhone and laptop computer, purportedly to fix the devices, for several hours before giving them back to Ms. Markaryan.

164. Ms. Markaryan's computer and iPhone contained highly private and sensitive photographs and videos that were improperly accessed by Clery.

165. Ms. Markaryan was a minor under the age of 18 for the majority of her time at Kent School, during which time Clery was accessing her PEDs.

V. KENT SCHOOL HAD A DUTY TO PROTECT ITS STUDENTS AND EMPLOYEES FROM CLERY.

166. Kent School has publicly admitted that it failed to safeguard the health and safety of the Kent School community from Clery's improper and illegal conduct. In an October 11, 2024 letter to the Kent School Community Members, Jeffrey D. Cataldo, the Associate Head, Chief

Financial Officer and Chief Operating Officer of Kent School, wrote, “The School’s commitment to keeping students and all members of our community safe, including the protection of their personal information, is a top priority. We fell short in this commitment as it relates to the Dan Clery matter. We take this matter very seriously and understand the lasting impact it has on students and Kent School community. I want to personally apologize to all who have been affected by these events...”

167. On October 9, 2024, Jeffrey Cataldo wrote to “All Impacted by the Spring 2022 Breach of Trust at Kent School” to report that after Clery’s employment was terminated, “[c]ertain actions were taken to strengthen our monitoring of the School’s network, [and] controls were adopted and/or strengthened to control employee use of the School applications...”

168. Michael Hirschfeld, the Head of Kent School, wrote to plaintiffs and the members of the Class on April 18, 2023 to advise them that Clery “had accessed and may have copied personal photographs and/or videos from your computer...” He too apologized, stating “I am very sorry that this happened. Our commitment to the safety of our community extends to cyber security and data protection, and we are doing all that we can to resolve this matter and to prevent it from happening again.”

169. In a Zoom meeting with affected current and former students held on October 14, 2024, Jeffrey Cataldo admitted “[O]ur systems processes had controls at the time in which Mr. Cleary was accessing information. Clearly those controls were not good enough... He, in that position, had certain permissions to allow him to do his job, which should have carried more controls. And that was an error.”

170. Also on October 14, 2024, Kent School, through its employees, agents, and/or authorized representatives, admitted that Clery “managed” and “cared for” the Kent School

network “and as part of that work, he would often engage in a support role with both students and adults who may be having issues accessing the network or doing certain things.” Defendant further admitted that there had been “a massive shortcoming” in Kent School’s failure to implement reasonable industry standard cybersecurity controls, and that its cybersecurity controls “were not good enough,” that Kent School committed an “error,” and that their protocols violated the “industry standard.”

171. Kent School’s admissions indicate its awareness that it had a duty to take all reasonable steps to keep its students safe, including a duty to supervise Clery and impose controls over his conduct to safeguard against his using high-level access to Kent School’s computer network to spy on members of the Kent School community and access and steal their private and personal data, photos, videos, and emails.

172. Kent School’s admissions also indicate its awareness of how severely plaintiffs and the Class members were damaged by the misappropriation of their private images and data.

173. During the October 14, 2024 Zoom meeting, when asked whether and how Kent School was going to advocate for the student victims with respect to Clery’s criminal prosecution, Jeffrey Cataldo stated, “I do believe there’s a role for the school, and that is, you know, we stand for those harmed, the student victims at Kent School, and we want to make sure the Court recognizes how severe that harm is...”

174. Moreover, Kent School was on notice by at least the spring or summer of 2022 of the precise behavior that would later form the basis of the criminal prosecution against Clery. Kent School’s failure to take any action or undertake any sort of inquiry into KC’s initial complaint demonstrated extreme and egregious indifference to the privacy interests of its students and staff and disregard for their safety and well-being.

175. The degree to which safety measures to protect against the type of computer misconduct engaged in by Clery could and should have been implemented is further demonstrated by the fact that Clery himself made a statement to the police when they arrived at his house to execute the search and seizure warrant offering recommendations for safeguards Kent School could implement to prevent the transfer of personal information to Kent School's servers by bad actors in the future. Clery's recommendations were captured on a police body camera.

176. Plaintiffs and the Class have been severely damaged as a result of Kent School's failure to take action to safeguard their personal information from its employee, Clery. Plaintiffs and Class members have suffered a devastating invasion of privacy. They have lost exclusive control over their highly sensitive images and information that continue to be vulnerable to exploitation and misuse.

177. To that end, in an attempt to limit such future misuse and exploitation of their highly personal data, plaintiffs and Class members will be required to hire data removal specialists to scour the internet and remove their personal information. Plaintiffs and Class members, teens and young adults when their intimate photographs and videos were accessed, stolen, and copied by Clery, a middle-aged man with an interest in voyeurism and pornography, have suffered sexual exploitation and abuse as a result of the invasion of their privacy.

CLASS ALLEGATIONS

178. Plaintiffs bring claims for negligence, invasion of privacy, computer privacy violations, statutory computer privacy violations, recklessness, and negligent infliction of emotional distress, as a class action pursuant to the Connecticut Rules for the Superior Court, Conn. Practice Book §§ 9-7 and 9-8.

179. Plaintiffs seek certification of a Class defined as follows:

All current or former students of Kent School who had personal information stored on an electronic device, including photographs, videos, and email communications that was accessed, transferred, copied, retained or utilized at any time by Daniel Clery, without their knowledge or consent from June 2019 through February 2023. (“Class Period”).

180. Plaintiffs reserve the right to modify or refine the definitions of the Class or add subclasses based upon discovery of new information.

181. Excluded from the Class are: (a) any Judge presiding over the Action and members of their staff, as well as members of their families; (b) defendant Kent School and its predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which defendant Kent has a controlling interest, as well as Kent’s agents, officers, and directors; (c) persons who properly execute and file a timely request for exclusion from the Class; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (e) counsel for plaintiffs and Defendant; and (f) the legal representatives, successors, and assigns of any such excluded person.

182. Ascertainability. The proposed Class is readily ascertainable because it is defined using objective criteria which allow class members to determine if they are a member of the Class. Further, much, if not all, of the Class has been identified through forensic analysis of Kent School’s servers and Clery’s work laptops conducted by Vancord and the State Police investigation.

183. Numerosity. The Class is so numerous that joinder of individual members herein is impracticable. There are at least 70 students or former students who have been identified to date. Courts have recognized that cases involving 40 or more plaintiffs meet the numerosity requirement. *See Artie’s Autobody, Inc. v. Hartford Fire Ins. Co.*, No. X08CV030196141S, 2006 WL 2730143, at *3 (Conn. Super. Ct. Aug. 30, 2006), aff’d sub nom. Artie’s Auto Body, Inc. v.

Hartford Fire Ins. Co., 287 Conn. 208, 947 A.2d 320 (2008) (“[t]here is no ‘magic number’ that satisfies the numerosity requirement.... a respected commentary on class action law suggests a presumption of sufficient impracticability and numerosity should arise when the putative class exceeds 40 members.” *Citing* 1 Conte & Newberg, *Newberg on Class Actions*, § 3.5 (4th ed.2002).

184. Commonality. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class members, including:

- a) Whether Kent School owed a duty of care to plaintiffs and the Class;
- b) Whether Kent School, by its employees, agents and/or representatives, was negligent in failing to take appropriate measures to ensure the safety and well-being of plaintiffs and the Class;
- c) Whether Kent School, by its employees, agents and/or representatives, was negligent in failing to put in place appropriate security measures to prevent Clery from accessing plaintiffs’ and the Class’s private and personal information;
- d) Whether Kent School, by its employees, agents and/or representatives, was negligent in failing to supervise Clery’s actions with respect to his ability to access, transfer, and retain the private and personal photos, videos and communications stored on the personal laptops of plaintiffs and the Class;
- e) Whether Kent School took appropriate steps to ensure the safety and security of plaintiffs and the Class after it received notification that Clery was accessing private information on a Kent School staff member’s laptop in 2022;
- f) Whether Kent School, by its employees, agents and/or representatives, was negligent in retaining Clery as a Kent School employee with the highest IT access, and in failing to terminate Clery’s employment after it received notification that Clery was accessing private information on a Kent School staff member’s laptop in 2022;
- g) Whether Kent School’s failure to take steps to ensure the safety and security of its students after receiving notification that Clery was accessing private information on a Kent School staff member’s laptop in 2022 was reckless;
- h) Whether plaintiffs and the Class suffered losses and damage as a direct and proximate result of Kent’s negligence;

- i) Whether plaintiffs and the Class suffered losses and damage as a direct and proximate result of Kent School's recklessness;
- j) Whether plaintiffs and the Class are entitled to common law punitive damages as a result of Kent School's recklessness;
- k) Whether the access, transfer, copying and retention of plaintiffs and the Class's private and personal data constituted an invasion of privacy;
- l) Whether the disclosure of plaintiffs' and the Class's private photographs and videos would be highly offensive to a reasonable person;
- m) Whether Kent School, by its employees, agents or representatives, violated Gen. Stats. §§ 53a-251 and 52-570b;
- n) Whether Kent School's actions in violation of Gen. Stats. §§ 53a-251 and 52-570b were willful and malicious;
- o) Whether Daniel Clery functioned within his role as an authorized agent or apparent agent of Kent School in furtherance of the interests of Kent School.

185. Typicality. Plaintiffs' claims are typical of the claims of the other members of the proposed Class. Plaintiffs and members of the Class suffered injuries as a result of Kent School's alleged wrongful conduct that is uniform across the Class.

186. Adequacy. Plaintiffs fairly and adequately represent and will protect the interests of the Class. Plaintiffs have retained counsel competent and experienced in the litigation of claims involving invasion of privacy, school negligence, and sexual exploitation and abuse, and in the litigation of class actions. Plaintiffs have no interest that is antagonistic to those of the Class, and Kent School has no defenses unique to plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the resources and experience to do so. Neither plaintiffs, nor plaintiffs' counsel have any interest adverse to those of the other members of the Class.

187. Substantial Benefits. This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this

controversy and joinder of all members of the Class is impracticable. The prosecution of separate actions by individual members of the Class would impose heavy burdens upon the courts and Kent School, would create a risk of inconsistent or varying adjudications of the questions of law and fact common to members of the Class, and would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and will promote uniform decision-making.

188. For the foregoing reasons, class certification is appropriate under Conn. Practice Book §§ 9-7 and 9-8.

189. On March 9, 2026, the Court (Klau, J.) certified a class defined to consist of “all current or former students of Kent School who had personal information stored on an electronic device, including photographs, videos, and email communications that were accessed, transferred, copied, retained or utilized at any time by Daniel Clery, without their knowledge or consent from September 2016 through February 2023 (“Class Period”).

190. On that same date (March 9, 2026), the Court appointed the named plaintiffs to serve as class representatives.

191. The Court limited the class action to the following claims, issues or defenses:

- a) As to Count One (Negligence), (i) whether Kent School owed the plaintiffs a duty of care during two time periods: (1) September 2016 to Spring/Summer 2022, and (2) Spring/Summer 2022 through February 2023, (ii) the nature and scope of any such duty of care, and (iii) whether Kent School breached any such duty;
- b) As to Count Four (Recklessness), if Kent School owed the plaintiffs a duty of care and breached such duty, whether Kent School acted recklessly;

- c) As to the CUTPA claim, (i) whether Kent School was engaged in trade or commerce with respect to its alleged negligence concerning Daniel Clery; and (ii) whether Kent School's alleged conduct in employing Clery, giving him access to the plaintiffs' computers and electronic devices, failure to maintain reasonable cybersecurity protocols for a school environment, and failure to act to protect the plaintiffs' information once it knew of the breach constitutes unfair and/or deceptive trade practices under CUTPA.

CAUSES OF ACTION

FIRST COUNT: NEGLIGENCE
(against Kent School on behalf of Plaintiffs and the Class)

1-191. Paragraphs 1- 191 are incorporated and made paragraphs 1-191 of this First Count.

192. Kent School, an educational institution entrusted with the well-being of its students, owed a duty of care to its students to safeguard the privacy and security of their digital information, including their private and personal photographs, videos, and emails when that information was in the custody and control of Kent School, its employees, agents and/or representatives.

193. Kent School's computer servers and networks were vulnerable to exploitation as a result of Kent School's failure to properly supervise Clery, failure to establish proper procedures to regulate the safety of information on its servers and networks, and failure to investigate Clery's conduct. Members of Kent School's senior administration have acknowledged as much after the arrest of Clery. Clery himself stated that Kent School could have and should have done more to secure and fortify its system.

194. Kent School, by the acts and omissions of its administrators, IT Department Head, teachers, and other staff members, who were employees or agents of Kent School acting within the scope of their employment or agency with Kent School and in furtherance of the interests of Kent School, was negligent in failing to take reasonable measures to ensure the safety and well-being of its students, including plaintiffs and the Class, in one or more of the following ways:

- a) By failing to establish an appropriate system to monitor access by members of its IT staff, including Clery, to its computer network and/or the personal computing devices of students;
- b) By failing to provide adequate oversight and supervision of its employees whom it had a duty to supervise, including Clery, with respect to access to its computer network and/or the personal computing devices of students;
- c) By failing to implement and maintain a system of controls necessary to safeguard regulated information;
- d) By permitting Clery to introduce his personal server into Kent School's work environment;
- e) By allowing Clery unrestricted access to the Kent School network without implementing a cybersecurity program containing administrative, technical and physical safeguards for the protection of sensitive personal information of the plaintiffs;
- f) By providing students, including the plaintiffs, IT services relating to their PEDs and the Kent School network when Kent School knew, or had reason to know, that there were no protective measures in place to safeguard the students' sensitive personal information;
- g) By allowing Clery to take possession of the students' PEDs when it knew, or had reason to know, there were no protective measures in place to safeguard the students' sensitive personal information or to prevent installation of programs, applications, or the like, on their PEDs without their knowledge or consent;
- h) By failing to investigate or take any steps to secure the digital data, including photos, videos, and emails, of Kent School community members including plaintiffs and the Class, after receiving KC's report of Clery's misappropriation of her personal digital data in the spring or summer of 2022;
- i) By permitting Clery to retain his highest-level IT access even after receiving a report of his misuse of his position and misappropriation of personal digital data in the spring or summer of 2022;
- j) By failing to terminate Clery's employment after receiving a report of his misuse of his position and misappropriation of personal digital data in the spring or summer of 2022; and

- k) By failing to implement and maintain an appropriate process for offboarding employees with privileged access to Kent School's computer network, including Clery.

195. By failing to take appropriate measures as described above, Kent breached its duty of care to plaintiffs and the members of the Class.

196. As a result of Kent School's negligence, Clery was able to access, transfer, copy, and exercise possession over the private and personal information, including digital photographs, videos, and email communications, of plaintiffs and the Class over a period of years.

197. The negligent failure(s) of Kent School, as set forth above, was a substantial factor in causing the damages that plaintiffs and the Class have suffered, as set forth herein.

198. As a result of Kent School's negligence, plaintiffs and the Class have suffered and will in the future continue to suffer anxiety, concern, and distress over how their highly private and personal information was used by Clery, and whether and to what extent it has been, or in the future may be, distributed to others.

199. As a result of Kent School's negligence, plaintiffs and Class have suffered and will, in the future, continue to suffer significant personal injuries, losses and damages, including but not limited to:

- a) Severe emotional distress from the invasion of their privacy, including anxiety over how their highly private and personal information has been and will be misused and exploited; stress and anxiety resulting from fear that the theft of their sensitive personal information will impair their ability to obtain future employment; fear for their safety; and loss in their ability to trust and relate to authority figures, technological support staff, institutions, and friends and partners;
- b) Sexual exploitation and abuse from the illegal access, use and dissemination of their highly private photographs, videos, and information;
- c) Monetary loss in that they will need to hire data removal specialists to determine the extent to which their private and personal information has been disseminated and to mitigate current and future exposure.

SECOND COUNT: RECKLESSNESS
(against Kent School on behalf of Plaintiffs and the Class)

1-193. Paragraphs 1-193 of the First Count are incorporated and made paragraphs 1-193 of this Second Count.

194. Even after a Kent supervisor was notified in the spring or summer of 2022 by a female employee (KC) that Clery was viewing her personal photos on a school-issued laptop without her consent to do so, Kent School intentionally failed to investigate Clery's actions, did not revoke Clery's highest-level IT administrator access, and did not to put into place appropriate controls to prevent unauthorized access to the private information on the laptops of students and staff to which Clery had unimpeded access.

195. The deliberate decision of Kent School and its senior administrators not to take any action to investigate Clery or to increase IT security controls after being specifically notified in the spring or summer of 2022 of Clery's abuse of his position and authority to engage in improper and illegal access, misuse, and misappropriation of personal data was wilful, wanton, malicious, and/or done with reckless disregard for the safety and privacy of the Kent School students it had a duty to protect.

196. Kent School's deliberate indifference to protection against invasion of privacy for students, most whom were female, created a heightened risk of sexual abuse and sexual exploitation.

197. As a result of Kent School's wanton, wilful and reckless conduct, plaintiffs' and the Class's personal and private photos, videos, and emails were misappropriated and plaintiffs' and the Class's privacy was invaded, causing plaintiffs and the Class to suffer and continue, in the future, to suffer serious and permanent emotional, psychological, and bodily injuries arising directly from the invasion of privacy, including

- a) Severe emotional distress from the invasion of their privacy, including anxiety over how their highly private and personal information has been and will be misused and exploited; stress and anxiety resulting from fear that the theft of their sensitive personal information will impair their ability to obtain future employment; fear for their safety; and loss in their ability to trust and relate to authority figures, technological support staff, institutions, and friends and partners;
- b) Sexual exploitation and abuse from the illegal access, use and dissemination of their highly private photographs, videos, and information;
- c) Monetary loss in that they will need to hire data removal specialists to determine the extent to which their private and personal information has been disseminated and to mitigate current and future exposure.

198. As a result of Kent School's willful, wanton, malicious, and/or reckless conduct, plaintiffs and the Class are entitled to recover their actual damages and common law punitive damages.

**THIRD COUNT: VIOLATIONS OF GEN. STAT. § 42-110a, ET SEQ. ("CUTPA")
(against Kent School on behalf of Plaintiffs and the Class)**

1-199. Paragraphs 1-199 of the First Count are incorporated and made paragraphs 1- 199 of this Third Count.

200. At all times relevant to this Complaint, the defendant was engaged in trade or commerce as defined in General Statutes § 42-110a(4).

201. Beginning in approximately 2016, the defendant engaged in a continuous course of illegal and corrupt business activity over many years, including:

- a) committing computer crimes in violation of General Statutes § 53-451(b)(1) through (7) actionable through General Statutes § 53-452;
- b) allowing Daniel Clery to commit computer crimes in violation of General Statutes § 53-451(b)(1) through (7) actionable through General Statutes § 53-452;
- c) failing to create, maintain and/or comply with a written cybersecurity program containing administrative, technical and physical safeguards for

the protection of personal or restricted information including sensitive personal information of its minor students, including the plaintiffs, that conforms to an industry recognized cybersecurity framework, as described in Public Act No. 21-119 and/or in compliance with industry standards;

- d) breaching the implied covenant of good faith and fair dealing contained in the agreements between the defendant and the minor plaintiffs' parents which was accompanied by the aggravating circumstances described in this Complaint;
- e) violating General Statutes § 17a-101a when they knew or had reason to know that minor students, including plaintiffs, were being sexually exploited by a school employee, and they failed to report such sexual exploitation; and
- f) failing to warn or notify the plaintiffs of data breaches in violation of General Statutes § 36a-701; and,
- g) violating the plaintiffs' privacy rights.

202. The actions, conduct, and practices of the defendant described above constitute unfair and deceptive business practices in violation of General Statutes § 42-110b.

203. As a result of the defendant's unfair and deceptive business practices, the plaintiffs have suffered ascertainable losses including sexual exploitation, emotional distress, personal injuries, and economic losses

FOURTH COUNT: INVASION OF PRIVACY
(against Kent School on behalf of Individual Plaintiffs).

1-194. Paragraphs 1-194 of the First Count are incorporated and made paragraphs 1-194 of this Fourth Count.

195. Plaintiffs had a reasonable expectation of privacy in their personal photographs, videos, and communications stored on their computers and other digital devices, including the cloud.

196. Clery's access to plaintiffs' personal information was facilitated and enabled by Kent School. Kent School employed Clery for 23 years in its IT Department, increasing his level of responsibility and network access to the highest levels. As part of his duties as Network and Systems Administrator, Kent School provided Clery with the authority and ability to regularly gain access to student and staff computers. Clery used this access to transfer the personal information of plaintiffs to Kent School's servers and to his own electronic devices. Clery continued to enjoy this access after Kent School was put on notice of his misuse and misappropriation of KC's personal information. Clery could not and would not have had access to plaintiffs' personal information but for the authority granted to Clery by Kent School.

197. Kent School failed to secure and safeguard plaintiffs' privacy in their personal information, including but not limited to highly sensitive photographs and videos.

198. As a result of Kent School's actions and omissions, plaintiffs' privacy was invaded by its employee and authorized agent, Clery.

199. The disclosure of plaintiffs' personal and private information -- including but not limited to the accessing, viewing, transferring, retaining, and utilizing of plaintiffs' private photographs and videos, many of them depicting minors -- by Kent School (through its employee and authorized agent) would be, and is, highly offensive to a reasonable person.

200. The disclosure of plaintiffs' private information, including their photographs and videos, was not of legitimate concern to the public.

201. As a direct result of Kent School's conduct, plaintiffs' right of privacy has been invaded and plaintiffs have suffered and will, in the future, continue to suffer significant personal injuries, losses and damages, including but not limited to:

- a) Severe emotional distress from the invasion of their privacy, including stress and anxiety over how their highly private and personal information has been and will be misused and exploited; stress and anxiety resulting from fear that the theft of their sensitive personal information will impair their ability to obtain future employment; fear for their safety; and loss in their ability to trust and relate to authority figures, technological support staff, institutions, and friends and partners;
- b) Sexual exploitation and abuse from the illegal access, use and dissemination of their highly private photographs, videos, and information;
- c) Monetary loss in that they will need to hire data removal specialists to determine the extent to which their private and personal information has been disseminated and to mitigate current and future exposure.

**FIFTH COUNT: COMPUTER CRIMES, CONN. GEN. STAT. §§ 53a-251, 52-570b
(against Kent School on behalf of Individual Plaintiffs)**

1-193. Paragraphs 1-193 of the First Count are incorporated and made paragraphs 1-193 of this Fifth Count.

194. By his actions as aforesaid, Clery, acting with the authority provided him by Kent School, engaged in the crime of misuse of computer system information, in violation of Gen. Stats. § 53a-251(e) in that

- a) as a result of his accessing or causing to be accessed a computer system, he intentionally made or caused to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system;
- b) he intentionally or recklessly and without authorization took data intended for use by a computer system, whether residing within or external to a computer system, or intercepted residing within a computer system;
- c) he knowingly received or retained data obtained as set forth in sub-paragraphs a & b of this paragraph 194; and/or

- d) he used or disclosed data he knew or believed was obtained in violation of sub-paragraphs a & b of this paragraph 194.

195. Clery's access to plaintiffs' personal information was facilitated and enabled by Kent School. Kent School employed Clery for 23 years in its IT Department, increasing his level of responsibility and network access to the highest levels. As part of his duties as Network and Systems Administrator, Kent School provided Clery with the authority and ability to regularly gain access to student and staff computers. Clery used this access to transfer the personal information of plaintiffs to Kent School's servers and to his own electronic devices. Clery continued to enjoy this access after Kent School was put on notice of his misuse and misappropriation of KC's personal information. Clery could not and would not have had access to plaintiffs' personal information but for the authority granted to Clery by Kent School.

196. Kent School knew that its high-level employee, Clery, was improperly accessing the personal information of members of the Kent School community and intentionally allowed him to continue to do so.

197. Kent's actions in allowing Clery to engage in the conduct described herein were wanton, willful and/or undertaken in reckless disregard of its obligations to its students, including plaintiffs.

198. Kent School aided and abetted Clery's misuse of plaintiffs' computer system information.

199. Plaintiffs have suffered and will, in the future, continue to suffer actual damages as a result of Kent School's conduct in facilitating Clery's misuse of their computer system information, including

- a) Severe emotional distress from the invasion of their privacy, including anxiety over how their highly private and personal information has been and

will be misused and exploited; stress and anxiety resulting from fear that the theft of their sensitive personal information will impair their ability to obtain future employment; fear for their safety; and loss in their ability to trust and relate to authority figures, technological support staff, institutions, and friends and partners;

- b) Sexual exploitation and abuse from the illegal access, use and dissemination of their highly private photographs, videos, and information;
- c) Monetary loss in that they will need to hire data removal specialists to determine the extent to which their private and personal information has been disseminated and to mitigate current and future exposure.

200. Plaintiffs are entitled to recover their actual damages resulting from Kent School's participation in causing the computer privacy violations described above pursuant to Gen. Stats. §52-270b(c).

201. Kent School's conduct as aforesaid was willful and malicious, entitling plaintiffs to recover treble damages pursuant to Gen. Stats. §52-270b(c).

202. Plaintiffs are further entitled to recover their attorney's fees and costs in prosecuting this action pursuant to Gen. Stats. §52-270b(e)

**SIXTH COUNT: NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS
 (against Kent School on behalf of Individual Plaintiffs).**

1-195. Paragraphs 1-195 of the First Count are incorporated and made paragraphs 1-195 of this Sixth Count.

196. As a result of the negligence of Kent School, plaintiffs' private and personal photographs, videos, and emails were misappropriated by Clery and their privacy was invaded, causing plaintiffs severe emotional distress.

197. Kent School's negligent conduct created an unreasonable risk of causing emotional distress to plaintiffs.

198. Plaintiffs' emotional distress was a foreseeable consequence of Kent School's negligent conduct.

199. Plaintiffs' emotional distress was severe enough that it might result in illness or bodily harm to plaintiffs.

200. Kent School should have realized that its conduct involved an unreasonable risk of causing plaintiffs severe emotional distress and should have understood that such emotional distress might result in illness and/or bodily injury.

201. Kent School's conduct was extreme and outrageous.

202. Kent School negligently inflicted emotional distress on plaintiffs.

203. As a result of Kent School's negligent infliction of emotional distress, plaintiffs have suffered and will, in the future, continue to suffer significant personal injuries, losses and damages, including but not limited to:

- a) Severe emotional distress from the invasion of their privacy, including anxiety over how their highly private and personal information has been and will be misused and exploited; stress and anxiety resulting from fear that the theft of their sensitive personal information will impair their ability to obtain future employment; fear for their safety; and loss in their ability to trust and relate to authority figures, technological support staff, institutions, and friends and partners;
- b) Sexual exploitation and abuse from the illegal access, use and dissemination of their highly private photographs, videos, and information;
- c) Monetary loss in that they will need to hire data removal specialists to determine the extent to which their private and personal information has been disseminated and to mitigate current and future exposure.

DEMAND FOR RELIEF

Plaintiffs, on behalf of themselves and members of the Class, claim monetary damages in excess of fifteen thousand dollars including:

1. Compensatory damages for plaintiffs' and the Class's losses and injuries;
2. Common law punitive damages;
3. Punitive damages pursuant to Gen. Stat. § 42-110g;
4. Attorney's fees and costs pursuant to Gen. Stats. § 42-110g(d)
5. Actual damages pursuant to Gen. Stats. § 52-570b(c);
6. Treble damages pursuant to Gen. Stats. § 52-570b(c);
7. Attorney's fees and costs pursuant to Gen. Stats. § 52-570b(e);
8. Such other relief as the Court deems appropriate.

BY:

/s/ Jennifer B. Goldstein Juris No. 410497

David S. Golub, Juris No. 023810
Jennifer B. Goldstein, Juris No. 410497
Jennifer Sclar, Juris No. 446689
SILVER GOLUB & TEITELL LLP
One Landmark Square, 15th Fl.
Stamford, CT 06901
T: (203) 325-4491
F: (203) 325-3769
dgolub@sgtlaw.com
jgoldstein@sgtlaw.com
jsclar@sgtlaw.com

/s/ Joel T. Faxon Juris No. 410829

Joel T. Faxon, Juris No. 410829
FAXON LAW GROUP, LLC
59 Elm Street
New Haven, CT 06510
T: (203) 624-9500
jfaxon@faxonlawgroup.com

Co-Counsel for Plaintiffs

CERTIFICATION

This is to certify that on April 15, 2026, a true copy of the foregoing was delivered electronically and/or by regular mail to the following counsel and pro se parties of record and that written consent for electronic delivery was received for all counsel who were electronically served:

Daniel L. Schwartz
Howard Fetner
Lindsey A. McCarthy
DAY PITNEY LLP
One Stamford Plaza
263 Tresser Boulevard
Stamford, CT 06901
Tel: (203) 977-7300
dlschwartz@daypitney.com
hfetner@daypitney.com
lmccarthy@daypitney.com

For defendant: The Kent School Corporation A/K/A Kent School

/s/ Jennifer B. Goldstein Juris No. 410497
JENNIFER B. GOLDSTEIN



State of Connecticut Judicial Branch Superior Court E-Filing

**Attorney/Firm:** SILVER GOLUB & TEITELL (058005)**E-Mail:** KWOOD@SGTLAW.COM [Logout](#)[Hide Instructions](#)**You have successfully e-filed!**

Instructions: The information about the item you filed is on this confirmation page. You must print a copy of this page for your records. Choose **Print This Page** at the top of the page to print your copy.

Choose **E-File Another Pleading/Motion/Other on this Case** to go back to the **Select a Motion** page to choose another document name and file another document.

Choose **Return to Superior Court E-Filing Menu** to go back to the menu page.

Choose **Return to Case Detail** to look at the documents filed in this case or to file a reclaim in this case.

[Print This Page](#)

Confirmation of E-filed Transaction (print this page for your records)

Docket Number:	UWY-CV-25-6084708-S
Case Name:	LEARY, OLIVIA Et Al v. KENT SCHOOL CORPORATION A/K/A KENT SCHOOL
Type of Transaction:	Pleading/Motion/Other document
Date Filed:	Apr-15-2026
Motion/Pleading by:	SILVER GOLUB & TEITELL (058005)
Document Filed:	146.00 AMENDED COMPLAINT Consolidated & Amended Class Action Complaint
Date and Time of Transaction:	Wednesday, April 15, 2026 2:39:10 PM

[E-File Another Pleading/Motion/Other document on this Case](#)[Return to Civil / Family Menu](#)[Return to Case Detail](#)