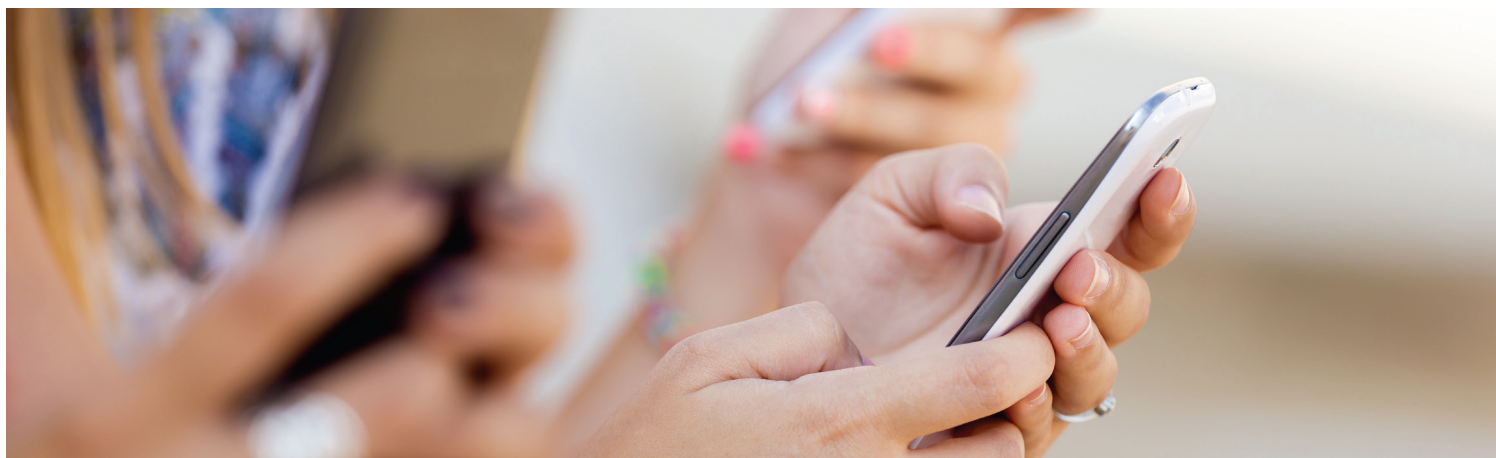# Creating a Healthy Digital Environment for 21st Century Learners

The Impact of Quality Leadership in Ventura County Office of Education
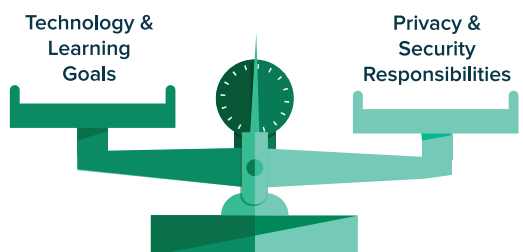
*By Marsali Hancock, President of iKeepSafe and
Dr. Robert Dillon, Director of the BrightBytes Institute*

BrightBytes **iKEEPSAFE**

UNDERSTANDING THE 21ST CENTURY LEARNING ENVIRONMENT

In too many places, digital privacy, safety, and security is the domain of the few, and is unacknowledged by most. When it is discussed, conversations in school districts often lack the complexity needed to build the essential structures and systems. This reality cannot continue because we live in a digital culture; online and offline worlds intersect across all areas of our lives. For children, this means what happens at school appears online, and what happens online appears at school. As much as schools have worked to make the safety of physical learning environments a top priority, it is time for schools and districts to protect their digital learning environments as well. This includes protecting personally identifiable information, passwords, network security, and data shared with third parties. It is no longer feasible for school districts to wait for an attack, breach, or mistake in data privacy to repair the security fabric of the district.

Accomplishing this doesn't mean saying no to innovative pedagogy and technology-rich learning, but rather, balancing technology and learning goals with privacy and security responsibilities. It is about protecting the back door while building a second floor. Schools are destined to transform, but only with good communication, careful planning, and sustainable processes can education organizations support all of these moving parts at once. Traditionally, educators have always worked together to protect students, and as education technology evolves, it is critical that stakeholders continue to come together to achieve a safe, healthy, and supportive digital learning environment. School systems with confident and skilled leaders will have a significant advantage in bringing these conversations into fruition.

Consider what it means to be a 21st century student submerged in a daily digital lifestyle. In the morning, you awake to your cell phone alarm. You pick up the phone, and check your text messages and social media sites for updates from your friends, family, and public figures you follow. Next, you use your phone to check the weather and to decide what to wear. While getting ready for school, you listen to your favorite song or watch the latest video game review. You head to school, listening to music and playing games on your phone. You arrive at school with various

Technology & Learning Goals — Privacy & Security Responsibilities

devices, such as computers, tablets, and even smartphones. You provide user information by logging in to several different educational software applications. Periodically, you check your phone, and witness digital dramas between your friends, acquaintances, and often yourself. On the way home, you pick up where you left off with your game. Upon arriving home, you access your teacher's website to check homework assignments, and possibly even complete some of these online. Throughout your day, each of these digital interactions follows you.
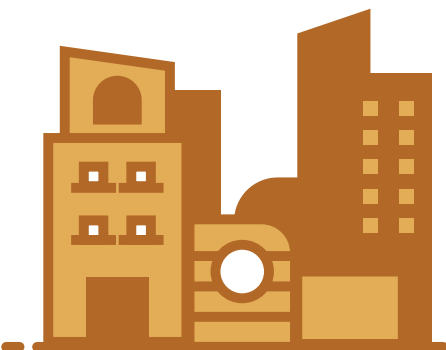
Meanwhile, your parents worry about your privacy and try to protect you. Teachers seek out the best new digital tools to meet your needs. Curriculum Directors encourage new tools necessary to meet learning goals. Technology Directors invest resources to ensure these new curriculum tools work within the capacity of the schools' network. School Counselors support you and your friends through digital drama, while they try to help students and protect their confidential information. School Principals search for ways to best use digital tools to support learning, and wonder how to prevent and respond to digital incidents. School board members want to keep their schools out of legal trouble and still provide an excellent education for all.

This work doesn't stop at the district level; it continues to service agencies and county offices, and then to state education and legislative officials. These officials can truly lead the way on this work because they cross-pollinate resources and ideas for security when incidents develop in one school or district. Service agencies and county offices become key communicators across the region allowing all to learn and grow from issues, as well as help everyone avoid making the same mistakes.

VENTURA COUNTY RESPONDS TO A SHIFTING LANDSCAPE

The landscape of student data privacy and safety is becoming more expansive and complex each year. Schools do not resolve these issues organically, or without a conscious effort. Quality leadership is necessary to maintain a positive and balanced environment. Stephen Carr, Chief Technology Officer of the Ventura County Office of Education (VCOE), exemplifies this type of leadership.

Carr initially focused on how to raise the awareness of Ventura County schools about the growing complexities of data privacy and security in the K-12 education space. The work over the next few years would coalesce around fostering a positive digital culture across districts. Carr partnered with iKeepSafe™, as they had worked with districts in this area for many years. Both iKeepSafe and VCOE knew that this concept was one that
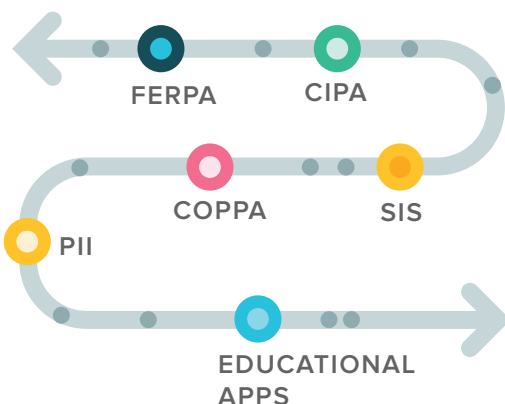
would have support on the surface, but various issues surrounding the topic are thorny and require strong leadership and an unwavering focus on communication, trust, and relationship building to make consensus a reality.

Carr's leadership allowed for this work to move through its various stages of implementation, from awareness to conversation, and from action planning to implementation. Carr's leadership strengths include his ability to inspire, value the ideas of others, and allow his team to "go" with their ideas as he supports them with resources, encouragement, and public acknowledgement. In addition, Carr has worked tirelessly to build the coalitions and networks necessary to fuel the work at VCOE and grow the conversation and ecosystem around the state. Carr has been a board member of the California Educational Technology Professional Association (CETPA) for the last 11 years, and a member of CETPA since 1998. He is currently CETPA's President-Elect. He has worked with the California State Department of Education and numerous other essential stakeholders around the state. Carr was recently named one of twenty education technology leaders nationwide to be honored by the National School Boards Association. In selecting Carr for the honor, the NSBA noted the work he's done to protect student privacy and promote responsible use of technology in education in a constantly changing digital world.

A JOURNEY TO A HEALTHY DIGITAL ENVIRONMENT

As these initial ideas began to blossom, Carr recognized that a positive digital culture across the county would only be possible if multiple stakeholders invested in the conditions necessary to promote an environment in which technology was used in a healthy and safe way. He knew that this type of culture would allow the benefits of technology to be actively embraced without reluctance, hesitation, or fear.

Carr and his team, including Dana Greenspan, Educational Technology Specialist, in cooperation with iKeepSafe, built upon three key areas as they worked to achieve this vision: relationships, trust, and credibility. They came to understand these as essential ingredients to build a coalition that could develop long-term solutions:

FERPA

CIPA

COPPA

SIS

PII

EDUCATIONAL APPS

- **Strong Relationships** were built as they worked to establish connections with various stakeholder groups across the county, focusing on the keys necessary to foster a positive digital culture. These individuals included Superintendents, Technology Directors, educators, administrators, board members, parents, students, and more. Each group was a part of genuine conversations that unearthed and communicated their interests and concerns.

- **Trust** was established as they delivered on promises and followed through on various action items to meet the needs of the stakeholders.

- **High-Level Credibility** was achieved as subject matter experts were engaged in all areas of the process.

This leadership style was modeled as they shifted from planning to action to address new significant student privacy laws. Carr brought together a leading law firm Fagen, Friedman, and Fulfrost (F3) with the California Educational Technology Professionals Association (CETPA), iKeepSafe, and the California County Superintendents Educational Services Association (CCSESA) to create the "Data Privacy Guidebook," which acts as a comprehensive resource for all California educators on digital safety and privacy law.

Once they accomplished this, they included iKeepSafe to explore opportunities to ease the heavy burden placed on school systems in California to comply with these laws. This partnership resulted in the development of iKeepSafe's California Privacy Badge, including an updated RFP, and the creation of their student privacy professional development and training certification.

VCOE used a privacy training workshop to gather support and momentum to pull together the key communicators needed to build an e-Safety task force around digital privacy, safety, and security. This task force was established to develop best practices and solve issues common to all of its districts around student privacy, safety, and security.

It should be noted that building a coalition in a large diverse county like Ventura requires excellent communication, courage to be direct about

needs, and an understanding of the areas of concern at a very deep level to provide specific examples that can be tailored to diverse audiences. One of the items that emerged from the early conversations about this work was that many Instructional Technology Directors and Chief Technology Officers felt tremendous pressure and angst on how to ramp up compliance to the breadth of data privacy needs in their district without stopping the positive momentum of technology integration currently going on in classrooms.

The task force would emerge with representation from 100% of its school districts and charters in the county, including a cross section of professionals with varied roles and responsibilities (Superintendents, Directors, Principals, Human Resources, Communications, and Instructional Technology Officers). This group would work in four areas:

- Board policies, including administration regulations and exhibits

- Programs to address data sensitivity (who has access to what student data and for what purposes)

- Product assessment and website content privacy

- Systems, security, and responses

Starting with policies is key to this work as it sets the foundation for the common language and expectations across all stakeholders in the organization. Good policies and programs, understood by everyone, increase the competence of all of those involved. This was made clear to them through their experience working with Simi Valley in 2011, a district within Ventura that was one of the first to employ iKeepSafe's Generation Safe™ program, successfully strengthening their digital safety practices across the district.

SCALING SUCCESS ACROSS AN ORGANIZATION

Ventura County continues to be a great example of leadership in the digital privacy space. They were able to bring the right groups together, grow the important conversations, and support educators in their efforts to innovate and protect their students. With the implementation of the Digital

Privacy, Safety & Security module, Ventura is taking their work to the next level, ensuring that stakeholders across the county are informed about the policies, programs, systems and responses related to digital privacy and safety and working to implement a unified vision. "Using the BrightBytes module, members of our eSafety task force will now be able to assemble a team for their own district that will help bring stakeholders together, document where each of these districts are, establish baselines, identify strengths and weaknesses, provide support for improvement, and develop clear, transparent channels of communication," explains Carr.
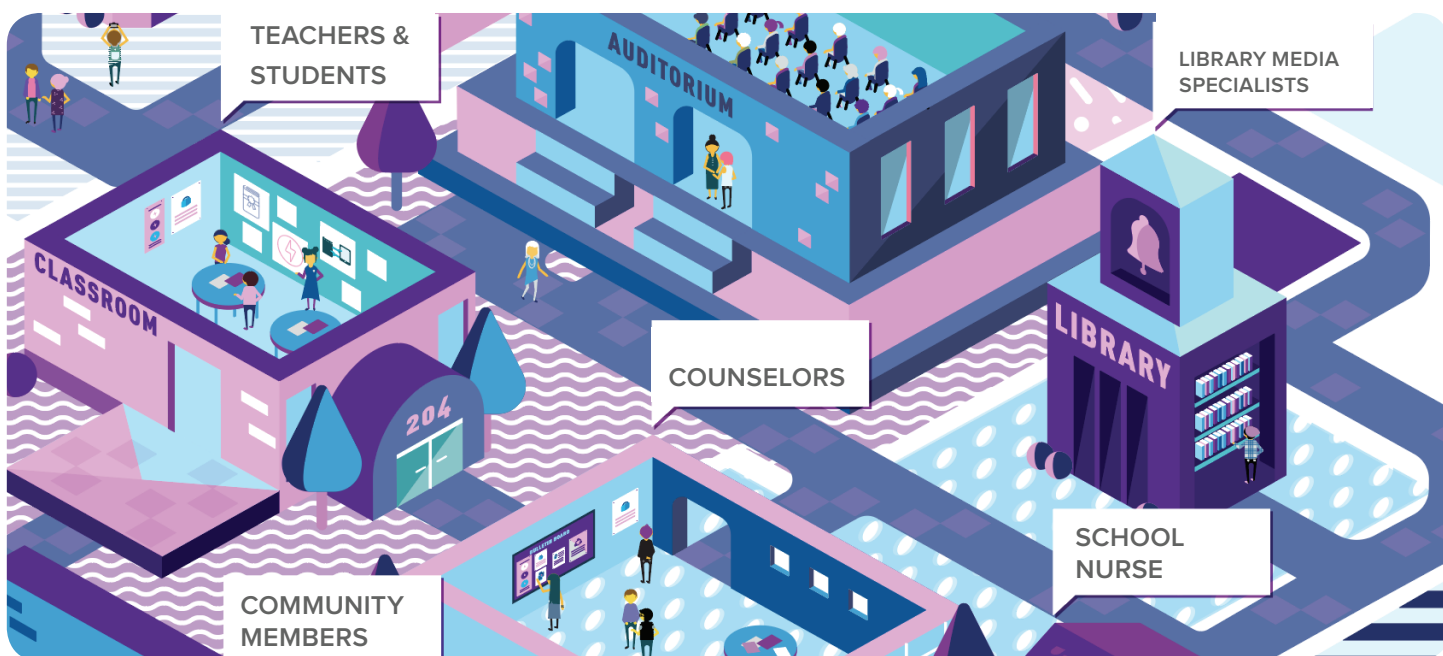
This was the motivation that drove iKeepSafe and BrightBytes to join together to build the Digital Privacy, Safety & Security module. The module provides the communication and guidance required to move school systems from a reactive environment, focused on risk management, to a healthy and positive digital culture. Bridging institutional silos can be a difficult process, but the module broadens the digital privacy conversation to a larger group of stakeholders, building the trust necessary for critical behavior changes across a system. Educators, Superintendents, Technology Directors, Curriculum Directors, and school administrators have different concerns and mindsets, but the platform helps to bridge these divisions.

Changing culture takes time, practice, cooperation, and constant communication. Though the needs of each school may vary, the module guides and supports district stakeholders through each essential stage of planning and implementation. Education leaders can determine, at a glance, which areas need additional support and resources. "When it comes to creating a healthy digital environment, it's not about arriving at a specific destination, it's about the journey, about working together to build a

> "
> *Using the BrightBytes module, members of our eSafety task force will now be able to assemble a team for their own district that will help bring stakeholders together, document where each of these districts are, establish baselines, identify strengths and weaknesses, provide support for improvement, and develop clear, transparent channels of communication."*

STEPHEN CARR
Chief Technology Officer
Ventura County Office of
Education (VCOE)

roadmap that will guide you through the complex, ever changing landscape of existing and new policies, requirements, and legislation" explains Marsali Hancock, President and CEO of iKeepSafe. The module creates an action plan and distributes communication and documents necessary to ensure that every district is both prepared to prevent digital incidents, and maximize innovative learning.

Employing Carr, Greenspan, and Ventura County's successful model, the Digital Privacy, Safety, & Security module acts as a catalyst for the development of these relationships, as well as the credibility required before new skill-building initiatives are implemented and sustained across districts. The expertise of iKeepSafe, BrightBytes, and their partners have been built into the module, to make success attainable for schools across the country. For years, iKeepSafe and their team have worked with experts in privacy, online safety, cybersecurity, public health, and law enforcement to develop a comprehensive body of knowledge around the complex digital environment. A significant amount of time and resources were placed into tying each valuable perspective into a cohesive framework. This knowledge informs digital tools like the Digital Privacy, Safety & Security module, as well as other programs, such as the iKeepSafe California Privacy Assessment and Generation Safe.
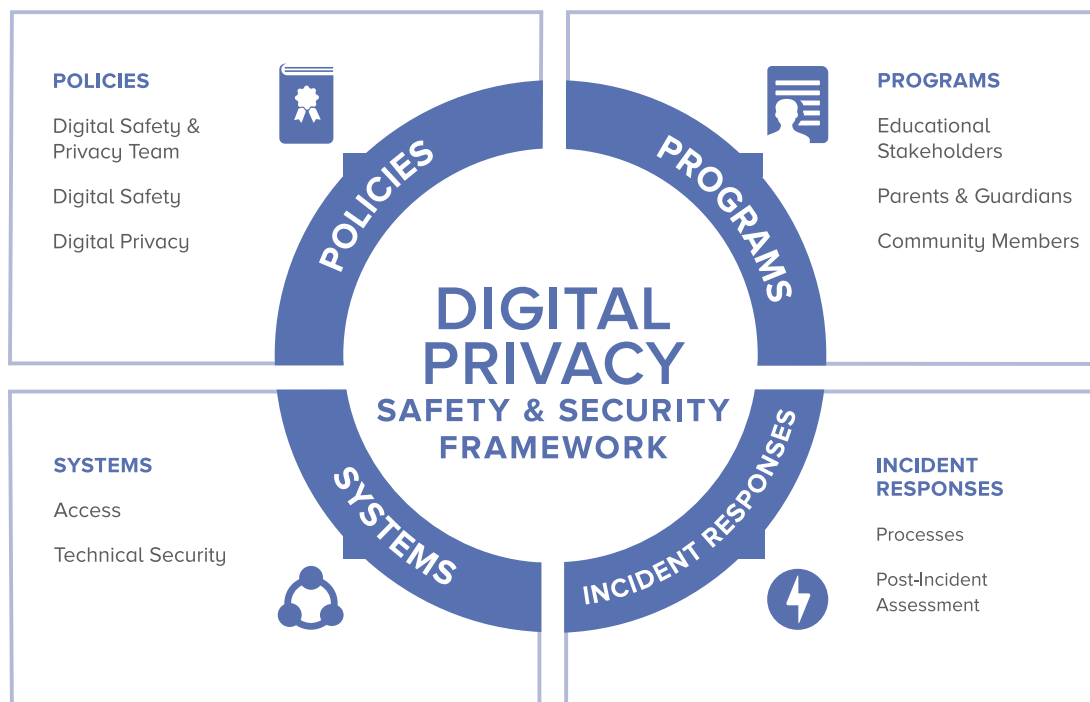
BrightBytes and iKeepSafe have examined the best research available on data privacy, safety, and security in order to build a module that education organizations can use to analyze their current reality, identify areas that need improvement, and obtain resources to make those improvements. BrightBytes is uniquely positioned to deliver a comprehensive solution to address the needs education organizations have balancing their technology and learning goals with their privacy and security responsibilities.
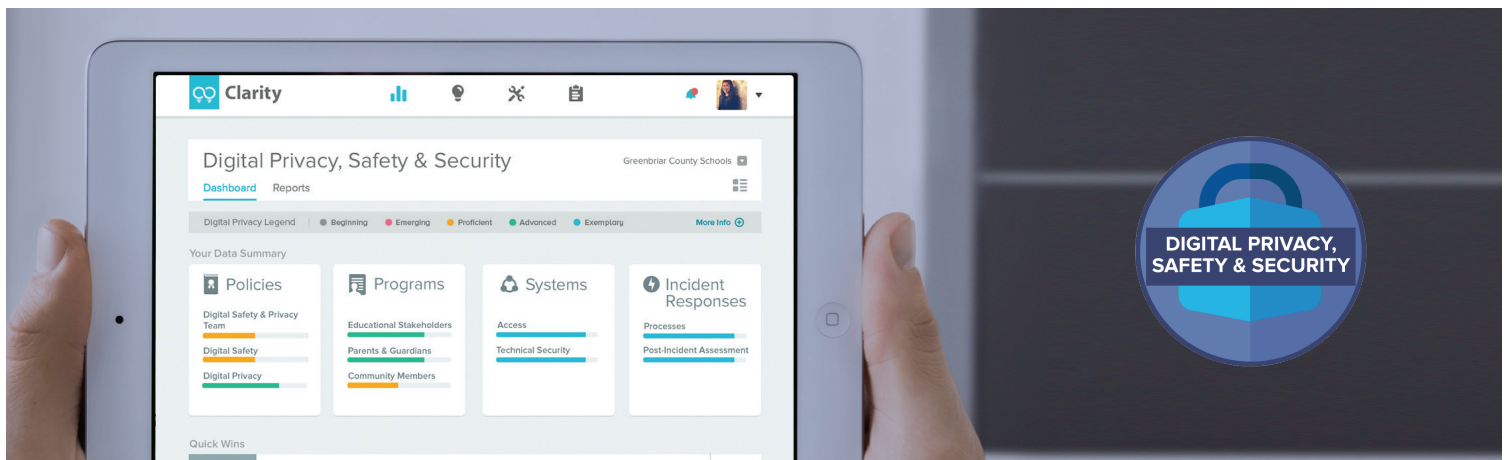
"

When it comes to creating a healthy digital environment, it's not about arriving at a specific destination, it's about the journey, about working together to build a roadmap that will guide you through the complex, ever changing landscape of existing and new policies, requirements, and legislation."

MARSALI HANCOCK
President and CEO
iKeepSafe

POLICIES

Digital Safety & Privacy Team

Digital Safety

Digital Privacy

PROGRAMS

Educational Stakeholders

Parents & Guardians

Community Members

SYSTEMS

Access

Technical Security

INCIDENT RESPONSES

Processes

Post-Incident Assessment

DIGITAL PRIVACY SAFETY & SECURITY FRAMEWORK

POLICIES — PROGRAMS — INCIDENT RESPONSES — SYSTEMS

THE DIGITAL PRIVACY, SAFETY & SECURITY MODULE

- Provides a clear picture of where you are on your journey

- Brings together a cross-functional team

- Scales work across schools, districts, and/or a state

- Analyzes digital culture against a research-based framework

- Visualizes results in an approachable, easy to understand format

- Keeps stakeholders informed of current and new legislation

- Provides best-in-class exemplars to support growth and improvement

- Creates a central repository of documentation and processes

- Delivers Quick Wins and Game Changers to make data actionable

An established leader in educational technology, their Clarity platform is currently improving teaching and learning in one in five U.S. schools and impacting more than 6.5 million students. BrightBytes' dedication to data science and making research accessible and actionable uniquely positions them to amplify the research and dedication of partners like iKeepSafe and others in the industry.

Using the module not only signals a commitment to due diligence and reducing liability, but also clarifies a framework sufficiently credible for schools to move forward with confidence. The module is instrumental in ensuring that schools are working to support the vision of creating a healthy digital environment.

Even with this preparation, schools and districts may still experience an incident to which they need to respond. Ventura County experienced this reality in early 2016, when their skills were put to the test. One of their districts' offices fell victim to a burglary. Several computers and hard drives containing sensitive student information were stolen. Though the incident was certainly unfortunate, Carr's leadership and communication with all schools, districts, and stakeholders in the county enabled the Superintendent to keep the situation under control. Not only was he able to optimally manage and support districts, but also provide communication plans and guidance to all key stakeholders, such as Superintendents, Principals, Tech Directors, and more.

Having all school systems connected by the BrightBytes Digital Privacy, Safety & Security module can help ensure a comparably unified and systematic approach to incident response. Ventura County's response included communicating to all stakeholders via the module, sharing information and establishing action steps with all responsible parties, coordinating with law enforcement, and fulfilling all mandatory data breach requirements. The incident response plan was implemented within hours of the breach, and within a few days all Superintendents in the county were notified of the occurrence. Additionally, Carr was able to provide further instruction surrounding data governance best practices in an effort to standardize quality data practices in every district and school within the county.

iKeepSafe and BrightBytes are continuing this momentum beyond Ventura County. Recognizing the complexity of this work for schools, districts, county officials, and others, BrightBytes and iKeepSafe are working together to make sure that youth can thrive in the digital culture that surrounds them. BrightBytes and iKeepSafe are dedicated to fostering and supporting great technology leadership in education, and the Digital Privacy, Safety & Security module is the first step in this ongoing process.

Digital privacy is an unwavering issue. It isn't something that will fade over time. Now more than ever, it is an issue that requires more conversations, more nuanced solutions, and more partnerships to manage the complex landscape. iKeepSafe has taken its deep bench of knowledge and research on this topic, and joined with BrightBytes, who supports this work through actionable data analytics, to advance the goal of helping all schools foster a healthy digital environment. Ventura County acts as an exemplary model of how great communication and leadership from key stakeholders across a school system can make this vision a reality.

ABOUT THE AUTHORS

iKEEPSAFE

MARSALI HANCOCK
President and CEO of iKeepSafe

Marsali Hancock is the founding president of iKeepSafe.org, an international non-profit network of more than 100 advocates that help track internet-connected devices' effects on children. Hancock develops tools to pinpoint quality digital practices for schools, industries, and families. Her primary focus is to identify critical policies, programs, and support structures needed to create a positive digital culture and to build the networks of support for youth to thrive.

BrightBytes INSTITUTE

DR. ROBERT DILLON
Director of the Research Institute at BrightBytes Institute

Dr. Robert Dillon has served the students and community of the Affton School District as Director of Technology and Innovation. He also has served as an educational leader in a number of public schools throughout the St. Louis area over the last twenty years. Dr. Dillon serves on the Leadership Team for Connected Learning, a St. Louis based organization designed to reshape professional development to meet today's needs. He is the author of two books on best practices in learning, *Leading Connected Classrooms* and *Engage, Empower, Energize: Leading Tomorrow's Schools Today.*

CONTRIBUTORS TO iKEEPSAFE'S DIGITAL PRIVACY, SAFETY, AND SECURITY SCHOOL SELF-ASSESSMENT, GENERATION SAFE 360™

BELINHA DE ABREU, PH. D.
Media Literacy Educator & Assistant Teaching Professor
Drexel University

LYNNETTE A. AVERILL, MS
Fulbright Scholar, Counseling Psychology Doctoral Student
University of Utah

DIANE BEAUDET
Vice President, Marketing Programs and Communications
Webroot Software, Inc.

JONATHAN COHEN, PH.D.
President, National School Climate Center

ANNE COLLIER
Founder and Executive Director
Net Family News, Inc.

LINDA CRIDDLE
President
LOOKBOTHWAYS, Inc.

JUSTIN T. FITZSIMMONS
Senior Attorney
National Center for Prosecution of Child Abuse National District Attorneys Association

NANCY V. GIFFORD
Special Counsel to iKeepSafe
Former US Assistant Attorney for the District of Connecticut (1989 — 2003)

STEVEN GILES
Elementary School Principal
Jordan School District

PENELOPE R. GLOVER
School Attorney
Atkinson, Andelson, Loya, Ruud & Romo

SAMEER HINDUJA, PH.D.
Co-Director, Cyberbullying Research Center School of Criminology and Criminal Justice Florida Atlantic University

JEFFREY L. HUNT ED.D.
Director, E-Learning The Institute for Online Learning Indian Prairie School District 204

LT. JOE LARAMIE
Administrator, Former Missouri ICAC Commander (retired)

MARY G. LEARY
Professor, The Catholic University of America Columbus School of Law

LINDA MCCARTHY
Technology Incubator, San Francisco Founder of OwnYourSpace

TAMMY MCGRAW, ED.D.
Director, Educational Technology Virginia Department of Education

SAM MCQUADE, MPA, PH.D.
CMS Graduate Coordinator, College of Applied Science and Technology Rochester Institute of Technology

CAPTAIN KIRK S. MARLOWE
Virginia State Police, Bureau of Criminal Investigation High-Tech Crimes Division

DAVINA PRUITT-MENTLE, PH.D.
Director, Educational Technology Policy, Research and Outreach Curriculum and Instruction

LINDA SHARP
Project Director, Cyber Security for the Digital District Consortium for School Networking

JULIA TAYLOR
Professional School Counselor, Wake County Public Schools Raleigh, NC

ROBYN TREYVAUD
Specialist Online Safety Consultant, Founder of CyberSafeKids

GLEN WARREN
Coordinator of Media Resources, Orange County (CA) Department of Education

THOMAS HUTTON
Associate Attorney, Patterson Buchanan Fobes Leitch & Kalzer, Inc., P.S

MICHAEL RICH, MD, MPH
Director, Center on Media and Child Health (CMCH) Boston Children's Hospital
Associate Professor, Harvard Medical School
Associate Professor, Harvard T.H. Chan School of Public Health

CHARLES LEITCH
Founding Principal, Patterson Buchanan Fobes Leitch & Kalzer, Inc., P.S

GWEN SCHURGIN O'KEEFE
CEO & Editor in Chief, Pediatrics Now

SUSAN KEYS, PH.D.
Special Advisor on Mental Health, Director of Research, Inspire USA Foundation

FRANK GALLAGHER
Executive Director, Cable in the Classroom

KERI L. HERRMANN, MD
Director
Pediatric Psychiatry Utah State Hospital

KATIE GREER
Internet/Digital Safety Expert, CEO, KL Greer Consulting