Training Course on Cybersecurity and Data Privacy for School Administrators

Professional Development Training Course Outline

Category	Educational Leadership and Management	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the digital age, where schools increasingly depend on technology to deliver education, secure administrative systems, and manage sensitive data, cybersecurity and data privacy have become critical priorities. School administrators are at the forefront of protecting educational institutions from cyber threats such as ransomware attacks, phishing scams, data breaches, and identity theft. Training Course on Cybersecurity and Data Privacy for School Administrators is specifically designed to empower school administrators with practical skills, regulatory knowledge, and strategic frameworks for creating and maintaining a secure digital environment across K–12 and higher education institutions.

As the threats to digital infrastructure evolve rapidly, it is essential that educational leaders are not only aware of potential vulnerabilities but also equipped to respond proactively. Through this comprehensive, hands-on course, participants will learn to mitigate risks, implement data protection policies, comply with privacy regulations like FERPA and COPPA, and foster a culture of cyber awareness among staff and students. Our training integrates real-life case studies, cutting-edge tools, and scenario-based simulations tailored for the educational sector.

Programme Curriculum

Training Course on Cybersecurity and Data Privacy for School Administrators

Introduction

In the digital age, where schools increasingly depend on technology to deliver education, secure administrative systems, and manage sensitive data, cybersecurity and data privacy have become critical priorities. School administrators are at the forefront of protecting educational institutions from cyber threats such as ransomware attacks, phishing scams, data breaches, and identity theft. Training Course on Cybersecurity and Data Privacy for School Administrators is specifically designed to empower school administrators with practical skills, regulatory knowledge, and strategic frameworks for

creating and maintaining a secure digital environment across K–12 and higher education institutions.

As the threats to digital infrastructure evolve rapidly, it is essential that educational leaders are not only aware of potential vulnerabilities but also equipped to respond proactively. Through this comprehensive, hands-on course, participants will learn to mitigate risks, implement data protection policies, comply with privacy regulations like FERPA and COPPA, and foster a culture of cyber awareness among staff and students. Our training integrates real-life case studies, cutting-edge tools, and scenario-based simulations tailored for the educational sector.

Course Objectives

1. Understand cybersecurity fundamentals in the education sector
2. Identify and manage digital threats targeting schools
3. Implement data privacy compliance with FERPA, COPPA, and GDPR
4. Establish a cybersecurity policy framework for school systems
5. Learn incident response and breach mitigation procedures
6. Promote cyber hygiene practices among staff and students
7. Conduct cyber risk assessments and audits
8. Explore the use of AI-driven cybersecurity tools
9. Develop password management and access control protocols
10. Address challenges of remote learning security
11. Integrate multi-factor authentication (MFA) in school systems
12. Train staff in cyber threat awareness and phishing simulations
13. Establish a data backup and disaster recovery plan

Target Audiences

1. School Principals
2. District Administrators
3. IT Managers in Education
4. School Board Members
5. Data Protection Officers
6. Compliance Officers in Schools
7. Academic Coordinators
8. Digital Learning Directors

Course Duration: 10 days

Course Modules

Module 1: Introduction to Cybersecurity in Education

- Define cybersecurity in a school context
- Types of common cyber threats in schools
- Importance of protecting digital infrastructure
- Key components of a cybersecurity program
- Understanding the administrator’s role
- *Case Study: Ransomware Attack on a Public School District*

Module 2: Data Privacy Regulations and Compliance

- Overview of FERPA, COPPA, and GDPR
- Legal responsibilities of schools
- Consent management for student data
- Policy creation and enforcement
- Penalties for non-compliance

- *Case Study: COPPA Violation in a Charter School*

Module 3: Cyber Threat Landscape in Education

- Identifying common threat actors
- Understanding malware and phishing
- Insider threats in schools
- Trends in K–12 cyber attacks
- Early detection indicators
- *Case Study: Phishing Attack Targeting School Staff*

Module 4: Developing a Cybersecurity Policy

- Elements of a strong school cyber policy
- Drafting acceptable use policies (AUP)
- Roles and responsibilities
- Policy communication and enforcement
- Policy review and updates
- *Case Study: Implementation of AUP in a High School*

Module 5: Incident Response Planning

- Creating an incident response team
- Step-by-step response plan
- Notification and documentation procedures
- Engaging law enforcement
- Post-incident recovery
- *Case Study: Data Breach in a Private School*

Module 6: Risk Assessment and Audits

- Conducting a cybersecurity risk audit
- Evaluating digital assets and threats
- Ranking vulnerabilities
- Tools for assessment
- Compliance checklist
- *Case Study: Audit Results Leading to Policy Overhaul*

Module 7: Password and Access Management

- Password policies and best practices
- Role-based access control
- Secure authentication methods
- Avoiding credential sharing
- Educating staff and students
- *Case Study: Breach Due to Shared Credentials*

Module 8: Cybersecurity in Remote and Hybrid Learning

- Securing virtual classrooms
- Safe use of third-party tools
- Home network security tips
- Monitoring online activity
- Cloud service protection
- *Case Study: Zoom-Bombing Incident During Online Class*

Module 9: Phishing and Social Engineering Defense

- Recognizing phishing attempts
- Creating awareness training
- Reporting suspicious emails
- Technical defenses
- Simulated phishing campaigns
- *Case Study: Phishing Simulation in a School District*

Module 10: AI and Automation in Cybersecurity

- Introduction to AI-powered tools
- Benefits and risks of automation
- Threat detection and response
- Automating audits and monitoring
- AI ethics in education
- *Case Study: AI Bot Detects Data Leak in School System*

Module 11: Physical and Network Security

- Securing school devices and servers
- Network segmentation strategies
- Physical access control
- Wi-Fi safety protocols
- Routine maintenance and updates
- *Case Study: Theft of Unsecured School Laptop*

Module 12: Backup and Disaster Recovery

- Planning for worst-case scenarios
- Backup frequency and types
- Cloud vs. on-site backup
- Restoration procedures
- Testing recovery plans
- *Case Study: Natural Disaster and Data Recovery Process*

Module 13: Cybersecurity Budget and Resources

- Allocating budget effectively
- Prioritizing tools and training
- Grants and funding opportunities
- Cost-benefit analysis
- Open-source security tools
- *Case Study: Budget Reallocation for Cybersecurity Upgrade*

Module 14: Building a Culture of Cyber Awareness

- Leadership's role in cyber culture
- Empowering teachers and students
- Embedding security in school values
- Celebrating cybersecurity month
- Feedback and continuous improvement
- *Case Study: Cybersecurity Awareness Week in Middle School*

Module 15: Future-Proofing School Cybersecurity

- Anticipating evolving threats
- Continuous learning and training

- Building long-term strategies
- Investing in new technologies
- Partnerships with cybersecurity firms
- *Case Study: Preparing for Next-Gen Threats Using Predictive AI*

Training Methodology

- Interactive instructor-led workshops
- Real-life case studies and problem-solving sessions
- Gamified quizzes and cyber drills
- Group-based scenario simulations
- Hands-on labs and tool demos
- Resource materials and templates provided

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com