Cybersecurity Pathway

This exciting new pathway of three course is the result of a joint effort between the Columbia County School System, the Richmond County School System, Fort Gordon, and Georgia Regents University. It has been approved by the Georgia Department of Education and is being offered at Greenbrier, Grovetown and Lakeside High Schools. The Cybersecurity courses are

- Introduction to Digital Technology (ITC 201-202)
- Introduction to Cybersecurity (ITC 203-204)
- Advanced Cybersecurity (ITC 205-206)

The Cybersecurity Pathway provides students with the computer and problem-solving skills necessary for success in the field of Cybersecurity. Students gain a background in digital technology that includes protecting networks from outside attacks and how to develop network level security policies.

ITC 201-202
Introduction to Digital Technology 11.41500 Prerequisite: None
Credit: 1 Grade Level: 9-12 Status: Elective
This course is designed for students to understand, communicate, and adapt to a digital world as it impacts their personal life, society, and the business world. Exposure to foundational knowledge in hardware, software, programming, web design, IT support, and networks are all taught in a computer lab with hands-on activities and project focused tasks. Students will not only understand the concepts, but apply their knowledge to situations and defend their actions/decisions/choices through the knowledge and skills acquired in this course. Competencies in the co-curricular student organization, Future Business Leaders of America (FBLA), are integral components of the employability skills standard for this course. Various forms of technologies will be highlighted to expose students to the emerging technologies impacting the digital world. (Textbook: Understanding Computers: Today and Tomorrow, Comprehensive © 2011, 13th Edition, Cengage, ISBN: 9780538748100)

ITC 203-204 11.481.00 Prerequisite: ITC 201-202 Credit: 1
Introduction to Cybersecurity Grade Level: 10-12 Status: Elective
This course is designed to provide students with the basic concepts and terminology of cybersecurity. The course examines how the concept of security integrates into the importance of user involvement, security training, ethics, trust, application of cybersecurity practices and devices, and best practices management. The fundamental skills cover internal and external threats to network security and design, how to enforce network level security policies, how to protect an organization’s information, and a broad range of other topics. Various forms of technologies will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills and practices, problem-solving, ethical and legal issues, and the impact of effective presentation skills are enhanced in this course to prepare students to be college and career ready. Employability skills are integrated into activities, tasks, and projects throughout the course standards to demonstrate the skills required by business and industry. Competencies in the co-curricular student organization, Future Business Leaders of America (FBLA), are integral components of the employability skills standard for this course. Introduction to Cybersecurity is the second course in the Cybersecurity career pathway of the Information Technology Career Cluster and primarily focuses on the National Cybersecurity Workforce Framework category Protect and Defend and the Computer Network Defense work roles. Students enrolled in this course should have successfully completed Introduction to Digital Technology.

ITC 205/206 11.48200 Prerequisite: ITC 203-204 Credit: 1
Advanced Cybersecurity Grade Level 11-12 Status: Elective
This course is designed to provide students with the advanced concepts and terminology of cybersecurity. The course explores the field of cybersecurity with updated content including new innovations in technology and methodologies. It builds on existing concepts introduced in Introduction to Cybersecurity and expands into malware threats, cryptography, organizational security, and wireless technologies. Various forms of technologies will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills and practices, problem-solving, ethical and legal issues, and the impact of effective presentation skills are enhanced in this course to prepare students to be college and career ready. Employability skills are integrated into activities, tasks, and projects throughout the course standards to demonstrate the skills required by business and industry. Competencies in the co-curricular student organization, Future Business Leaders of America (FBLA), are integral components of the employability skills standard for this course. Advanced Cybersecurity is the third course in the Cybersecurity career pathway in the Information Technology Career Cluster. Students enrolled in this course should have successfully completed Introduction to Digital Technology and Introduction to Cybersecurity.