Digital Strategy 2025

Introduction

In today's rapidly evolving digital landscape, it is crucial for educational institutions to embrace technology to enhance learning, operational efficiency, and communication. This digital strategy outlines the approach St Helens College and Knowsley Community College will take in adopting, integrating, and leveraging digital tools and platforms to achieve its academic, administrative, and security objectives. Key areas of focus include the integration of digital tools within the curriculum to enhance students' learning, cyber security, marketing and safeguarding. .

Vision and Goals

The goal of the digital strategy is to create a digitally empowered college environment where technology supports teaching and learning, enhances communication and marketing, ensures the safety of the college community, and safeguards the college's digital infrastructure. This strategy will be developed and implemented with active involvement from key stakeholders, including students, staff, and the wider community.

Key Objectives:

1. **Enhanced learning experiences.** Through the integration of digital tools, students will have more interactive and personalised learning experiences.
2. Harnessing **artificial intelligence (AI)** to enhance learning and improve efficiency and decision-making, while fostering a culture of innovation.
3. **Digital marketing** approaches that increase the College's visibility, attract prospective students, engage current stakeholders and supports the institution's overall mission and goals.
4. **Operational efficiencies** through the streamlining of administrative processes with digital solutions that will reduce manual workload, increase productivity and allow staff to focus on more strategic initiatives.
5. **Improved cyber-security and compliance**, through the implementation of robust cyber security and control measures, to protect the College's digital assets, ensuring data privacy and compliance with regulations.
6. **Enhanced safeguarding** by utilising digital safeguarding tools which will protect students and staff from online threats and ensure a safe learning environment.

Objective 1 – Enhanced Learning Experience

Curriculum and Digital Learning

Objective

To integrate digital tools into the curriculum, promote flexible learning environments, and enhance student engagement through technology.

Key Focus Areas:

Blended Learning: Adopt a blended learning model that combines face-to-face teaching with online resources, enabling students to access learning materials anytime and from anywhere. Implement platforms such as learning management systems (LMS) to deliver online content, assessments, and interactive activities.

Digital Literacy: Incorporate digital literacy into the curriculum, ensuring that students develop the skills necessary to use digital tools, software, and online resources effectively for academic and professional purposes.

Innovative Teaching Tools: Encourage the use of digital tools such as interactive whiteboards, online quizzes, and virtual labs to enhance the learning experience. Support curriculum teams in adopting these technologies through professional development programs.

Assessment and Feedback: Use digital tools for assessments, enabling online quizzes, digital submission of assignments, and automated grading where possible. Provide timely, digital feedback to students on their performance.

Collaboration Platforms: Implement collaboration tools such as Microsoft Teams to facilitate group projects, communication, and document sharing among students and faculty.

Key Deliverables:

- Adoption of an LMS to facilitate online learning and collaboration.

- Regular professional development for college staff on the use of digital tools.

- Integration of digital literacy into the core curriculum

Objective 2 - Artificial Intelligence (AI)

Objective

To leverage artificial intelligence (AI) to enhance learning, streamline administrative processes, and improve efficiency and decision-making, while fostering a culture of innovation, ethical use, and accountability within the college community.

Key Focus Areas:

AI-Enhanced Learning: Use AI to create personalised learning pathways for students, adapting to their individual needs and learning styles. Implement AI-driven tutoring systems to provide real-time feedback and support to students. Utilise AI to generate and curate educational content, ensuring it is up-to-date and relevant.

Administrative Efficiency: Implement AI to automate routine administrative tasks such as scheduling, grading, and data entry, freeing up staff time for more strategic activities. Use AI to analyse data and predict trends, helping to make informed decisions about resource allocation, student retention, and academic performance.

Data-Driven Decision Making: Leverage AI to analyse large datasets, providing insights that inform policy and strategy decisions. Implement AI tools for real-time reporting and dashboards, enabling quick and informed decision-making.

Ethical AI Use: Ensure AI systems are designed and monitored to minimise bias and promote fairness. Transparency in AI use and decision-making processes, to ensure accountability and ethical standards are upheld.

AI Literacy and Training: Provide training for staff on AI tools and their applications, ensuring they are equipped to integrate AI into their work. Incorporate AI literacy into the curriculum, preparing students for a future where AI plays a significant role.

Key Deliverables

- Development and deployment of AI-driven personalised learning platforms that adapt to individual student needs and learning styles.
- Automation of routine administrative tasks such as scheduling, grading, and data entry using AI technologies.
- Deployment of AI tools for predictive analytics to inform decisions on resource allocation, student retention, and academic performance.
- Development of a framework to ensure ethical use of AI, including measures to minimise bias, promote fairness, maintain transparency and accountability and consider environmental impact.
- Creation of training programs for staff on AI tools and their applications, and incorporation of AI literacy into the student curriculum.

Objective 3 - Digital Marketing

Objective: To leverage digital platforms to increase the College's visibility, attracts prospective students, engages current stakeholders, and supports the institution's overall mission and goals. This strategy will utilise data-driven insights, innovative technologies, and stakeholder collaboration to achieve measurable outcomes.

Key Focus Areas:

Social Media Marketing: Build a strong presence on social media platforms such as Facebook, Instagram, Twitter, TikTok, LinkedIn and YouTube to engage with students, alumni, and prospective applicants. Share success stories, events, and academic achievements regularly.

Website Optimisation: Continue to develop a user-friendly and mobile-optimised website that serves as the digital face of the college. Ensure that it is easy to navigate, has up-to-date content, and includes key features such as course information, an events calendar, and application portals.

Search Engine Optimisation (SEO): Implement SEO best practices to ensure that the College ranks highly on search engines for relevant queries, such as course offerings and campus activities.

Email Marketing Campaigns: Use targeted email campaigns to communicate with prospective students, alumni, and parents about important events, application deadlines, and news updates.

Analytics and Reporting: Use analytics tools to track the performance of digital marketing campaigns, identify trends, and measure return on investment (ROI).

Key Deliverables:

- Enhanced Online Presence. Achieve higher search engine rankings and increased organic traffic through effective SEO and content marketing strategies.

- Engaging Content: Develop and publish a variety of multimedia content, including blog posts, videos, infographics, and success stories, to keep the audience engaged and informed.

- Targeted Advertising Campaigns: Launch and manage digital advertising campaigns on platforms such as Google Ads, Facebook, and Instagram, aimed at attracting prospective students and increasing enrolment

- Social Media Growth: Increase followers and engagement on social media platforms by regularly posting relevant content, interacting with the audience, and running social media campaigns.

- Email Marketing Campaigns: Implement email marketing campaigns to nurture leads, keep current students and alumni informed, and promote college events and achievements.

- Analytics and Reporting: Utilise analytics tools to track the performance of digital marketing efforts, generate regular reports, and use insights to optimise strategies.

- Stakeholder-Generated Content: Encourage and facilitate the creation of content by students, staff, and alumni to ensure authenticity and relatability in marketing efforts.

- Continuous Improvement: Establish a process for regularly reviewing and updating the digital marketing strategy based on performance data, market trends, and stakeholder feedback.

Objective 4 – Operational Efficiency

Infrastructure and Technology Support

Objective: To provide reliable, secure, and scalable technology infrastructure that supports the college's digital ambitions and enhances the overall educational experience.

Key Focus Areas:

High-Speed Internet and Wi-Fi: Ensure robust and reliable Wi-Fi across the college campuses to support online learning, digital research, and administrative functions. Regularly upgrade infrastructure to meet increasing demand and maintain high performance.

Cloud Services: Transition to cloud-based solutions for data storage, software applications, and backup systems to enhance scalability, accessibility, and disaster recovery capabilities. Ensure compliance with data protection regulations.

Device Management: Implement a comprehensive device management strategy that supports BYOD (Bring Your Own Device) policies while ensuring security, compatibility, and efficient use of the College's digital platforms. Include regular updates and security patches.

Technical Support: Strengthen the College's IT helpdesk services to provide timely and efficient support for all technical issues, ensuring minimal disruption to learning and operations. Implement a ticketing system for tracking and resolving issues.

Key Deliverables:

- College-Wide High-Speed Internet Access: Deployment of high-speed internet and Wi-Fi across all campus areas, with regular performance monitoring and upgrades.
- Cloud-Based Data Storage and Backup Systems. Implementation of secure, scalable cloud solutions for data storage, software applications, and backups, ensuring easy access and robust disaster recovery.
- Accessible IT Support Helpdesk. Establishment of an easily accessible IT support helpdesk for students and staff, equipped with a ticketing system to ensure efficient issue resolution and minimal disruption.

Objective 5 - Cyber Security and Compliance

Cyber Security

Objective: To protect the College's digital assets from threats, ensure data privacy, and encourage a culture of cyber security awareness.

Key Focus Areas:

Network Security: Implement advanced firewall systems, intrusion detection, and real-time monitoring using AI and machine learning to identify and respond to threats more effectively. Maintain Cyber Essentials Plus accreditation.

Data Protection: Ensure compliance with data protection regulations such as the Data Protection Act, General Data Protection Regulation (GDPR) and CCTV Code of Practice. Encrypt sensitive data, implement multi-factor authentication (MFA), and adopt secure file-sharing practices. Regularly update all systems and software to protect against new vulnerabilities.

User Access Management: Implement strict access controls, ensuring that only authorised personnel have access to specific systems and data. Review access rights regularly to mitigate risks. Use AI to monitor and analyse access patterns for unusual activity.

Cyber Awareness Training: Provide mandatory cyber security training for staff and students to raise awareness about phishing attacks, password management, and secure internet use. Conduct regular phishing simulations to test and improve awareness and response.

Incident Response Plan: Develop a robust incident response plan to address potential security breaches, outlining steps for detection, response, recovery, and communication. Use AI-driven tools to enhance the speed and accuracy of incident detection and response.

Key Deliverables:

- Regular cyber security audits and penetration testing.
- Cyber security workshops and training for staff and students.
- Implementation of a college-wide data protection policy.
- Cyber Essentials Plus Accreditation
- Regular phishing simulations to test and improve cyber awareness.
- Continuous updates of systems and software to protect against emerging threats.

By incorporating AI and machine learning, emphasising the importance of regular updates, and including phishing simulations, this strategy aims to create a resilient and proactive cyber security posture for St Helens College.

Governance and Compliance

Objective: To ensure that the College complies with all legal and regulatory requirements related to digital services, data protection, and cyber security, while fostering a culture of compliance and accountability within the college community.

Key Focus Areas:

Digital and technology standards: Self-assessment of compliance with the DfE Digital and technology Standards in Schools and Colleges (updated January 2025) and identify and implement actions for improvement, where appropriate.

Data Protection Compliance: Adhere to data protection regulations such as GDPR by implementing robust data handling and privacy policies. Include regular training and awareness programs for staff and students to ensure everyone understands their responsibilities regarding data protection.

Cyber Security Audits: Conduct regular audits to assess compliance with cyber security policies and identify areas for improvement.

Policy Reviews: Regularly review and update the college's IT, safeguarding, and data protection policies to align with emerging risks and regulatory changes.

Key Deliverables:

- Annual Data Protection Compliance Audits
- Regular Updates to IT and Safeguarding Policies
- Legal Reviews of Digital Practices
- Compliance with the DfE Digital and technology Standards in Schools and Colleges (updated January 2025) and implementation of actions arising, if applicable.

Objective 6 - Safeguarding

Objective: To protect students from digital threats and on-line harm and ensure their well-being in both physical and online environments.

Key Focus Areas:

Online Safety Policies: Develop and implement a comprehensive online safety policy that outlines acceptable use of college technology, behaviour expectations, and protocols for reporting concerns.

Data Privacy: Ensure the privacy and security of student data by complying with data protection regulations, implementing secure data storage practices, and educating staff and students on data privacy best practices.

Digital Safeguarding Tools: Integrate digital tools and platforms that support safeguarding efforts, such as secure communication channels, reporting mechanisms, and monitoring systems.

Training and Awareness: Provide regular training for staff, students, and parents on safeguarding policies, recognizing signs of abuse or neglect, and how to report concerns. Promote a culture of vigilance and responsibility.

Incident Response: Develop and maintain a clear incident response plan for addressing safeguarding concerns, including procedures for reporting, investigating, and resolving incidents promptly and effectively.

Collaboration and Communication: Foster collaboration between safeguarding officers, educators, parents, and external agencies to ensure a coordinated approach to safeguarding. Maintain open lines of communication to address concerns and share best practices.

Policy Review and Improvement: Regularly review and update safeguarding policies and procedures to reflect new challenges, technological advancements, and feedback from stakeholders. Ensure continuous improvement in safeguarding practices.

Key Deliverables:

- Annual reviews of the online safety policy to ensure alignment with legal requirements.
- Development and enforcement of a comprehensive data privacy policy that aligns with GDPR and other relevant regulations.
- Regular training sessions for staff, students on safeguarding policies, recognizing signs of abuse or neglect, and reporting procedures.
- Real-time monitoring and incident management for safeguarding issues.
- Scheduled reviews of safeguarding policies and procedures to incorporate new challenges, technological advancements, and stakeholder feedback.
- Ongoing awareness campaigns to promote a culture of vigilance and responsibility among students, staff, and the wider college community.

Responsibilities

- The **Deputy Chief Executive Officer & Chief Finance Officer** has responsibility for developing the Strategy and is the SLT member responsible for digital technology.
- The **CEO / Principal and Accounting Officer** is responsible for supporting the development of the Strategy.
- The **Senior Leadership Team** is collectively responsible for the successful implementation of the Strategy.
- The **Head of IT** is responsible for ensuring an effective digital control environment.
- **All colleagues** who utilise IT technology are responsible for compliance with suite of IT and data protection policies and procedures, which underpin this Strategy and that constitute the internal control and risk management framework.
- Oversight of the delivery of this Strategy is undertaken by the **Finance, Resource and Commercial Committee** of the Governing Board and supported by the College's **assurance framework** (internal and external audit and Audit Committee arrangements).

Monitoring and Review

This Strategy will be reviewed and updated by the Deputy Chief Executive Officer & Chief Finance Officer on an annual basis. Following agreement by the Senior Leadership Team, it will be presented to the Finance, Resource and Commercial Committee, who will provide comment and make recommendations for approval by the Governing Board.

Conclusion

This digital strategy aims to create a secure, innovative, and engaging environment at St Helens College and Knowsley Community College where digital tools enhance learning, improve operations, and protect students and staff. By focusing on cyber security, marketing, safeguarding, and curriculum integration, the College will ensure that it remains at the forefront of digital transformation in education. Through ongoing evaluation and collaboration with all stakeholders, the College will continue to adapt and evolve its digital strategy to meet the needs of its community in the years to come.