parchment award™

Secure & Protect: Future Proof Your Credentials Management Ecosystem

Website: parchment.com
Email: info@parchment.com

parchment®
AN INSTRUCTURE COMPANY

parchment award™

Table of Contents:

Executive Summary

In a digital age where learner expectations are higher than ever, higher education institutions need a credential management approach that can keep pace. This white paper explores why transitioning to digital management solutions is crucial for addressing inefficiencies and fraud — all of which put institutions at risk of data breaches, operational delays, and compliance failures.

Key topics that will be covered include:

The growing problem of credential fraud, its causes, and the severe consequences it can have on the academic market.

How external threats, like cybercrime, affect higher education, including the most common types of attacks.

Challenges associated with relying on manual processes like spreadsheets and paper documents.

Best practices when switching from manual processes to a software solution that improves security, streamlines operations, and ensures compliance.

How credential management systems have enhanced efficiency, accuracy, security, and regulatory compliance.

Future-proofing credential management to avoid digital fraud and cybercrime.

Introduction

As digital transformation accelerates, technology is reshaping education. With the academic market embracing digital credentials, secure management is crucial to boosting security, improving the student experience, and maintaining institutional reputation.

What challenges highlight the need for safeguarded solutions?

Manual process inefficiencies: Outdated manual systems are prone to errors, data management headaches, and compliance issues.

Fraudulent credentials: Rising educational fraud in the UK, and similarly across Europe, jeopardises the integrity of academic qualifications – leading to legal, financial, and reputational fallout.[1]

Inconsistent credentialing: When institutions use different credentialing processes, it can create gaps in verification and make it harder to ensure security.

Rising cyber threats: Up to 86% of universities identified a breach or attack in the past year, putting sensitive data and institutional reputations at risk.[2]

Tougher compliance demands: Increasing regulations push institutions to uphold strict standards for data protection and credential accuracy.

Essentially, adopting digital solutions can streamline processes, enhance security, and ensure accuracy. However, achieving these benefits relies on embracing digital transformation and advanced credential management.

[1] https://www.theguardian.com/education/2021/feb/18/uk-degree-85-fake-university-websites-taken-down-in-five-years

[2] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex#

What is Risk Management and Why Does it Matter?

With their troves of sensitive data, academic institutions are prime targets for cyber threats. For example, higher education institutions are significantly more likely to experience cyber security incidents than the average UK business[2] Vulnerabilities like outdated software, lack of cybersecurity training, and weak response plans make them especially susceptible. That's where risk management comes in.

Risk management involves identifying, assessing, and mitigating potential risks to minimise their impact on an institution or its Student Information System (SIS). By proactively addressing threats, universities can safeguard their operations and data from potential threats and disruptions.

When it comes to digital credentials, risk management helps institutions:

- Identify potential threats and vulnerabilities within the system.
- Determine the severity of risks to prioritise resources effectively.
- Ensure adherence to relevant regulations and standards.
- Implement strategies to address identified threats proactively.
- Promote ongoing and effective risk management through continuous review.

Minimising institutional threats is essential for protecting universities from cyber risks and keeping data secure, making the credentialing experience better for learners and staff alike.

[2] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex#

Risk Management:

The Impact of Cybercrime & Security in the UK’s Education Sector

Hearing about rising cyber threats in the academic sector is one thing, but the numbers make it real. Here are key statistics on cybercrime in the UK's higher education sector, with similar impacts observed across institutions in Europe:

- **75%** reported needing additional resources to address these threats[3]
- **97%** of higher education institutions experienced breaches or attacks, almost twice the rate seen in primary schools[2]
- Just under **six in 10** universities suffered negative outcomes, such as financial or data loss[2]

Just under **six in 10** universities suffered negative outcomes, such as financial or data loss[2]

As of today, **100% of higher education institutions** report cybersecurity as a critical focus[2]

Why? Because:

- External bad actors pose significant risks as cyber attacks rise.
- Phishing, ransomware, DDoS attacks, and data theft are increasingly common threats.
- Cyber breaches lead to financial losses, data compromises, and operational disruptions.
- Leaders need to protect institutional integrity and maintain trust.

[3] https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities

Risk Management:
Credential Fraud in Education

Learners' rising demand for credentials has created a lucrative opportunity for fraudsters to exploit fake qualifications. Credential fraud includes using false or manipulated academic records, often from degree mills, to deceive employers or institutions. This issue is escalating in the education sector, with degree mills now generating $7 billion annually in global sales.[4]

Some of the most common examples of credential fraud in the UK's higher education system include:

- **Forged diplomas and certificates:** Fraudsters create and sell convincing counterfeit documents.
- **Misrepresentation of academic achievements:** Learners and others inflate grades and embellish academic records.
- **Manipulation of student records:** Unauthorised access leads to tampered academic histories, where external actors can alter grades and achievements without detection.

Degree mills now generate **$7 billion annually** in global sales, contributing to rising credential fraud.

Cases of counterfeit degrees and tampered transcripts can seriously tarnish an institution's reputation and spark legal troubles if negligence is involved. The costs of legal defence and remediation can also be hefty, putting a strain on resources and shaking up institutional trust and integrity.

[4] https://www.forbes.com/sites/emmawhitford/2023/02/21/how-thousands-of-nurses-got-licensed-with-fake-degrees/

Risk Management:

Universities Rely on Manual Processes for Credentials Management

Despite the rise in digital solutions and credentials, higher education leaders increasingly cite digital transformation as a challenge — climbing from 50% to 69% in just a year.[5] As a result, many institutions still cling to outdated methods for credential management, like spreadsheets and paper documents.

This leads to inefficiencies and risks, including:

- **Data management issues:** Scalability, real-time access, and timely updates are difficult to optimise, with a high risk of data loss.
- **Compliance and legal risks:** Keeping up with regulations like GDPR is challenging, heightening the risk of data breaches.
- **Operational inefficiencies:** Manual entry is laborious, error-prone, and less efficient than automated systems.
- **Limited data integration:** Manual systems often fail to integrate with other platforms, creating fragmented data and complicating analysis.
- **Increased costs:** Manual data handling is costly in terms of labour and time, compared to digital solutions.

The American University in Cairo

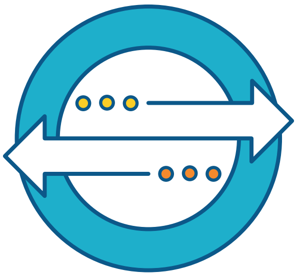
Case Study: What do these issues look like in practice? Consider the American University in Cairo (AUC). Their reliance on physical documents and international postal services led to long wait times and the risk of lost documents. After adopting Parchment, AUC eliminated these inefficiencies, providing students with instant access to their records and significantly improving satisfaction. This shift shows how digital solutions can streamline workflows and eliminate bottlenecks caused by outdated manual processes.

[5] https://www.holoniq.com/notes/2023-higher-education-digital-transformation-survey

The Need for EdTech Solutions

Given the inefficiencies of manual processes, growing credential fraud, and increasing cyber risks, universities are turning to educational technology and digital credential management to address evolving threats. EdTech is quickly proving to be a game-changer, with 41% of education leaders expecting it to **revolutionise communication with learners** over the next decade.[6] Another 36% see its potential in **streamlining institutional management.** Yet, despite its growing promise, education is still 'grossly under-digitised,' with less than 4% of global education spending going toward technology.

With increasing investments in digital solutions, digital credential management systems are becoming essential for institutions to efficiently issue, store, and verify academic credentials. And as educational technology gains traction, providers like Parchment are leading the charge with cutting-edge solutions for managing credentials and badges. These secure systems not only protect sensitive data but also deliver a seamless, user-friendly experience for students and academic institutions — transforming how credentials are handled in today's digital age.



41% of education leaders believe EdTech will revolutionize communication with learners over the next decade.

[6] https://assets.publishing.service.gov.uk/media/629f2065e90e070395bb3e4c/Future_opportunities_for_education_technology_in_England_June_2022.pdf

Digital Solutions for Credential Management

Credential management is transforming the way institutions handle and secure credentials today. Discover the advantages for higher education switching to a digital system:

1. Boosted Security

With cutting-edge encryption and strong authentication methods, digital credential systems greatly reduce the risk of unauthorised access and tampering — offering top-notch protection against fraud.

Parchment ensures data security by storing it in the cloud under local privacy laws and protecting academic documents with digital signatures, hosted sharing, and blockchain notarisation. This includes partnering exclusively with accredited education providers to guarantee legitimate, tamper-proof records.

2. Instant Access to Reporting

Say goodbye to delays. Digital systems like Parchment provide immediate access to up-to-date and accurate records, so information is always current and at stakeholders' fingertips.

3. Streamlined Administration

Automating credential issuance means less paperwork and fewer errors. This not only cuts down on administrative burdens but also allows institutions to allocate their resources more efficiently.

With Parchment, what used to take weeks — printing and posting thousands of transcripts — can now be done in minutes, all online. Plus, the self-service platform allows students to access and share their records at any time, reducing the need for institutional involvement and enabling secure back-to-source verification for employers.

4. Effortless Scalability

Managing large volumes of credentials becomes a breeze with digital systems that scale. Whether you're handling hundreds or thousands of students, there's no need to worry about physical storage limitations. As institutions aim to increase learner registrations, digital solutions like Parchment can seamlessly expand to accommodate more learners ensuring your credentialing process keeps pace with your growth.

5. Cost and Time Savings

Digital credentials slash costs related to printing, mailing, and storing physical documents. Plus, they minimise the need for extensive administrative work, significantly cutting the time spent issuing credentials.

Digital Solutions for Credential Management

6. Improved Compliance

Digital credential systems ensure compliance with data protection regulations like GDPR and FERPA. Plus, with built-in compliance tools, auditing and reporting are simplified.

7. Personalised Skills Representation

Institutions can create and customise digital badges and certificates to showcase individual achievements, reflecting each learner's journey.

8. Seamless Integration

Credential management systems integrate effortlessly with existing SIS and learning management systems. This creates a more unified and efficient workflow.

For instance, Parchment's modern REST APIs enable integration with any SIS, including Banner, Oracle (PeopleSoft Campus Solutions), SITS, Callista, and more. Parchment has been successfully implemented worldwide in partnership with leading universities, using web services and XML data standards for easy data export. As a result, institutions have noted improvements in student data accuracy and cleansing.

9. Sustainability

Reducing the need for paper-based processes contributes to sustainability efforts, promoting eco-friendly practices in line with modern environmental goals.

Implementation of Credential Management Systems

Once you've decided on digital credential management for your institution, what's next?

Choosing a system with strong security features and functionality tailored to your needs.
Key factors to consider include:

Customisation: Need flexibility? Ensure the platform can adapt to your unique requirements.

Vendor support: Pick a provider known for robust support during and after implementation.

Compliance requirements: Confirm the platform meets relevant regulations.

Scalability: Choose a platform that grows with your institution, handling future demands without frequent upgrades.

A global network: Opt for a platform with a global network to easily support student sharing across institutions, fostering trust and ensuring seamless learner mobility.

A few tips for successful implementation:

1. Use encryption and multi-factor authentication to keep credentials secure from unauthorised access.

2. Provide thorough training and highlight system benefits to win over stakeholders and ease the transition.

3. Plan your data migration carefully and leverage assistive tools for a smooth transfer of information.

4. Choose a platform with strong integration capabilities that grow with your needs and follow a well-planned migration strategy to seamlessly blend with your current systems.

Future Trends in Credentials Management

This is just the start of credential management in higher education. The future is brimming with exciting advancements, including:

A Lifelong Learner Account

The future of credential management is heading toward lifelong learner accounts, where individuals can securely store and share their academic achievements in one digital space. This gives students greater flexibility and control over their records throughout their education and career.

A Global Exchange of Credentials

As demand for a standardised credential system grows, a global exchange will allow learners to share qualifications across borders, opening doors to both regional and international opportunities. This global collaboration will make it easier for students to build an international academic profile and take achievements anywhere in the world.

Interoperability and Advanced Analytics

Looking ahead, emerging interoperability standards will enable seamless credential sharing and verification across different platforms, simplifying integration. At the same time, advanced analytics tools will provide deeper insights into credentialing trends, helping institutions refine their strategies.

Personalised Learning

Finally, and perhaps most importantly, personalised learning pathways will gain prominence — with credentialing systems increasingly supporting tailored achievements that reflect individual learning journeys.

Conclusion

A credentialing management platform with robust security protocols is crucial for higher education institutions to safeguard against evolving cyber threats, operational challenges, and credential fraud. Transitioning from manual to digital systems not only enhances security but also streamlines administrative processes.

Now is the time to embrace digital, and **Parchment** is here to make that transition seamless. With Parchment, institutions benefit from advanced security measures, including adherence to ISO 27001, SOC 2 Type II, and PCI DSS compliance. The platform also ensures:

- GDPR and CCPA compliance.
- Transparent data handling practices.
- Encryption.
- Regular security assessments.
- Secure international data transfers.
- Adherence to WCAG guidelines and provision of VPAT.

By choosing **Parchment**, you can effectively manage credentials and digital badges to reduce administrative burdens and focus on what matters most — empowering student success.

Book a demo to explore how Parchment can support your transition to a smarter, more secure credential management system.

Sources

1. https://www.theguardian.com/education/2021/feb/18/uk-degree-85-fake-university-websites-taken-down-in-five-years

2. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex#

3. https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities

4. https://www.forbes.com/sites/emmawhitford/2023/02/21/how-thousands-of-nurses-got-licensed-with-fake-degrees/

5. https://www.holoniq.com/notes/2023-higher-education-digital-transformation-survey

6. https://assets.publishing.service.gov.uk/media/629f2065e90e070395bb3e4c/Future_opportunities_for_education_technology_in_England_June_2022.pdf