What is Identity Protection?

White Paper

Studentnet Education Expert Series

September 2022

Dr Kate Lance

Studentnet

Studentnet CLOUDWORK®

Make the cloud yours®

Contents

Introduction

This paper, from the Studentnet Education Expert series, has been prepared for schools, particularly Cloudwork customers, with the aim of helping them improve their security posture.

As the chosen provider of identity protection and authentication services for many leading schools, Studentnet is in a position to provide unique insights into what works when it comes to identity and security in education.

Information security is not a task which is ever complete. Rather, it is a process requiring ongoing review and continuous improvement. Well thought-out policies and procedures, appropriately adapted to your environment, make it more likely the systems and structures to support excellent security practices will be maintained over the long term.

No school is the same as any other. Studentnet never takes a one-size-fits-all approach, and we are always happy to adapt to your school's unique context.

Kevin Karp
MD, Studentnet

1 Executive Summary

Schools differ from any other sort of organisation when it comes to technology and cybersecurity.

School IT staff support users across school communities from Kindergarten to Year 12 students, as well as staff, families and alumni, often numbering in the thousands, with vastly different levels of technical experience.

This white paper describes the three *contexts of school security* which require protection — operational infrastructure, personal privacy, and institutional reputation.

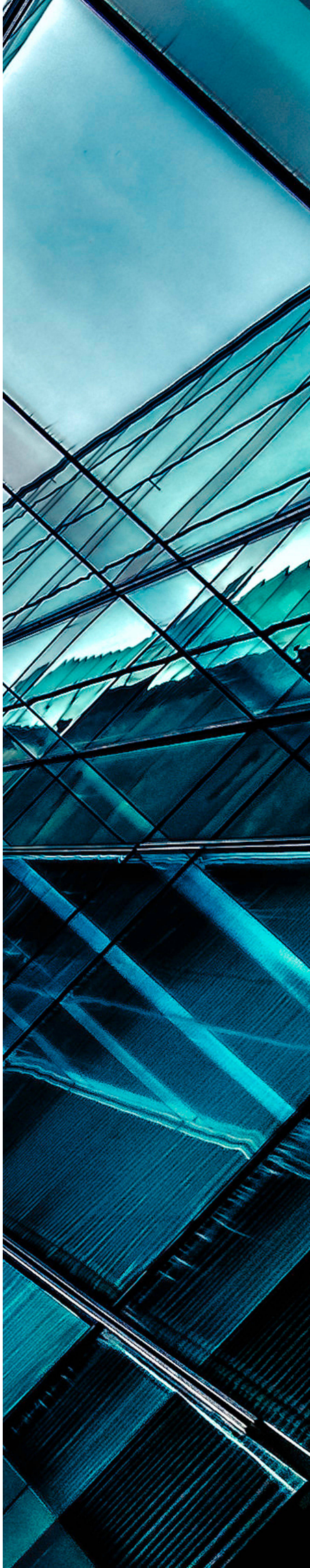
The protection of identity is shown to be fundamental in these security contexts:

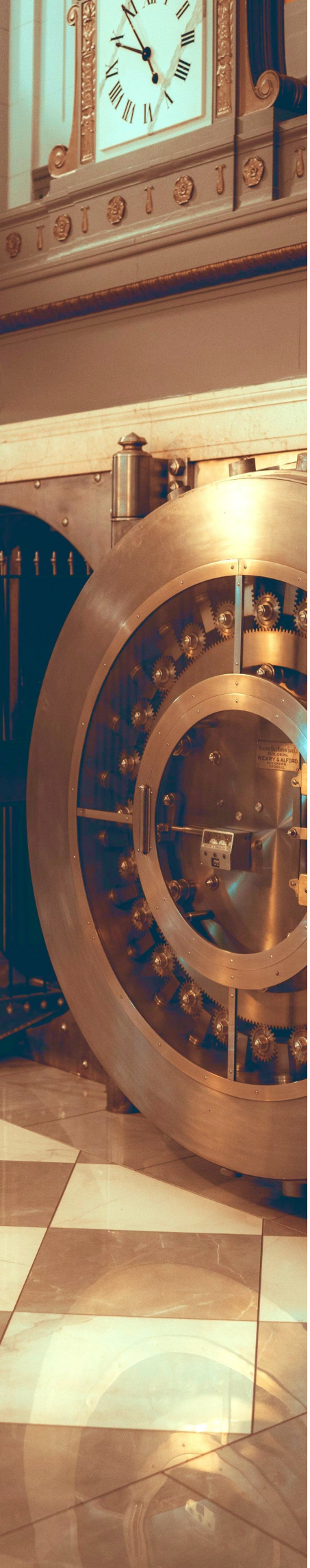
- **Operational identity**, which safeguards the new digital perimeters.
- **Personal identity**, which has life-long consequences across multiple school communities.
- **Institutional identity**, which is fundamental to school standing, influence and viability.

The three contexts of security interact with three *spheres of protection* that arise from integrated technical provisioning: the basic maintenance of accounts, the management of security and the protection of identity overall.

Identity protection arises from the measures that secure a school *at every level*, not simply at the stage of information technology.

Identity protection creates, monitors and safeguards the boundaries of an entire school — operationally, personally, and institutionally.





2 The Three Contexts

To fully protect a school, there are three distinct areas in which security must operate:

The Operational Context

The operational context covers the infrastructure that supports school functionality. It controls access to learning and administration facilities, authorises access to global academic resources, exercises duty of care, and provides long-term logging, auditing and oversight.

The Personal Context

The personal context protects the interests of the different school communities — students, staff, parents and alumni.

Schools are the repositories of the most confidential, sensitive and private information possible.

They maintain detailed digital records on private medical issues, legal obligations and financial details, and these must be rigorously safeguarded.

The Institutional Context

The institutional context covers the school's reputation and standing in the community. It must protect the school's influence and prestige, arising from academic performance, community engagement and brand recognition.

The safeguards for these contexts are not the same, and they are also *not simply a matter of information technology*.

Schools must protect themselves across their resources, their people, and their reputations.

The relationship between a school and its communities must be as secure as a bank.

3 Protecting Resources

In early online days, a school was kept secure by its network perimeter — the boundary between its internal network and uncontrolled external networks, such as the Internet. The perimeter permitted or denied access to infrastructure, facilities and confidential data.

Once it was patrolled via centralised logging, firewalls and physical datacentres, but in today's mobile Internet, that network perimeter is now the bare minimum of security.

Demands for remote work and always-on access have accelerated the massive move to the Cloud for providers.

But those digital services now rely utterly upon the proof of identity of whoever is seeking access.

Every time a school's resources are accessed, it can punch a hole in the perimeter and expose a school to risk.

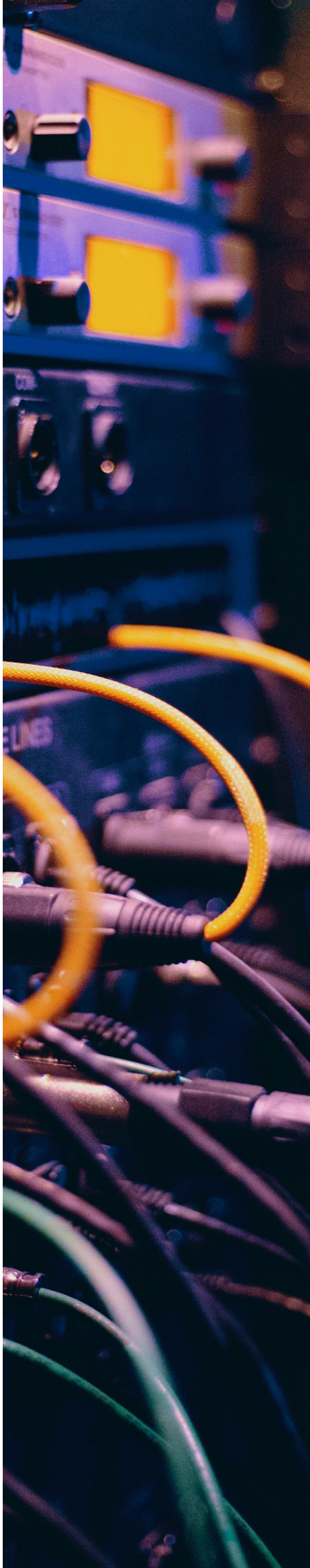
Passwords are not enough, and greater identity validation is necessary. At its simplest this is 'the name of your first dog,' but more serious safeguards are now widely used.

Multi-factor authentication is one, i.e. checking a user's identity against information only that user should have, such as an SMS token sent to their phone.

Zero Trust is another recent security framework. It requires all users, even those already inside the network, to be continually authenticated: nobody is trusted by default.

However, in all cases it is a user's *identity* that grants the right to access private, sensitive and privileged assets.

Identity is the new digital perimeter.



4 Protecting People

Once students were released from the limits of onsite computer-labs and provided with access from any device, anywhere, at any time, personal identity protection became a fundamental issue.

Attackers often focus their efforts on gaining access to accounts for use or resale. It is not surprising identity theft has become an increasingly massive and illegal industry.

In 2018-19, the estimated cost of identity crime in Australia was over three billion dollars, and in 2020-21, 11% of Australians suffered identity-based attacks, including theft of passwords, financial details and personal information, via malware, ransomware, and phishing fraud.[1]

Identity crime can have major consequences for targeted organisations, who not only incur the expense of investigating and remediating attacks, but, in the case of data and privacy breaches, face sometimes severe reputational damage.

Keeping the bad actors out all begins with identity.

Insurance companies recognise the scale of the problem and many now offer lower premiums to organisations that implement multiple and rigorous levels of identity protection, such as multi-factor authentication.

Hence, a school policy stance of *keeping the bad actors out* not only lowers costs, it also enhances reputation: and it all begins with identity.

1. https://get.eftsure.com.au/statistics/identity-theft-statistics

5 Identity and Timescales

Identity is not simply a function of birth certificates or passports. People take on different identities at different ages and in different jobs and, within a school, identities and their associated access rights will vary depending on roles.

Over time, students may become alumni, or staff, or the parents of the next generation of students. Staff may become parents, or parents become staff, and some roles and relationships may last a lifetime.

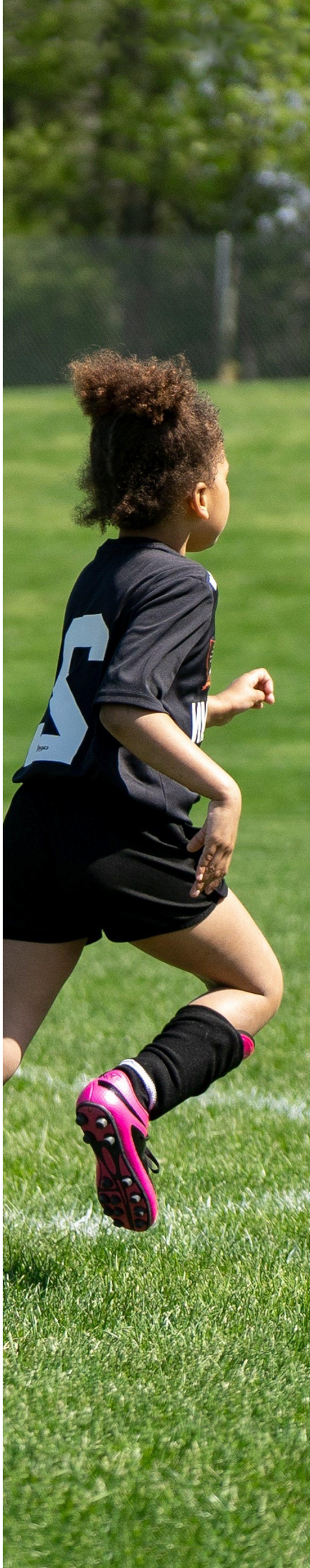
Students themselves will have multiple different identities that give them access to age-appropriate lessons, off-campus excursions, interest groups, specialised tuition, restricted software and more.

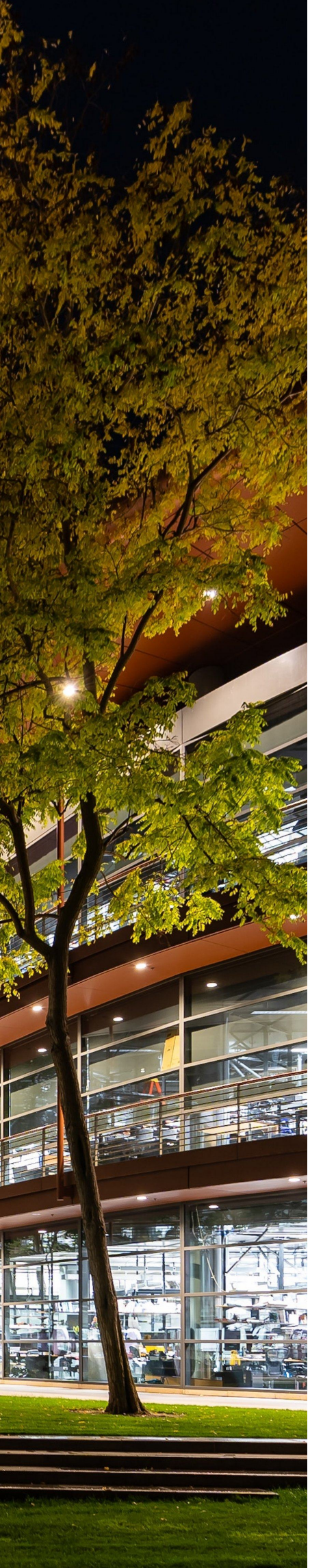
All of these will develop and change over the years of school, and often beyond.

School relationships are measured in decades, not years.

When children begin their education, it may be difficult for adults to visualise the life-long implications of them receiving their *first formally vetted and approved online identity*.

However, this identity must be professionally designed and safeguarded from the start, because school relationships with their users are measured in decades, not years, and identity protection must be continuous.





6 Protecting Institutions

From the first stages of the computing revolution of previous decades, everyone understood the essential roles played by hardware and software services and their administration, and the need to protect them.

More recently, we've recognised the importance of securing personal and confidential information, because privacy, and the breaches that lead to online fraud, have become a major social and economic issue.

But reputation? That falls into a third stage of awareness of the consequences of digital visibility. Commercial giants appreciate that reputational damage can threaten an organisation as much as poor performance.

Reputational damage can threaten an organisation as much as poor performance.

However, this is less well understood by schools. A school's reputation grows over time, based upon its influence and prestige arising from a number of factors:

Academic performance

Academic performance is a reflection of how well a school protects data such as exam questions, test results, homework submissions or student assessments.

Brand recognition

Brand recognition arises from direct promotion, with apps, websites, infrastructure and activities distinguished by school crests, links, mottos and taglines.

Community engagement

Community engagement grows out of trust, and provision of supporting services and connections for students, staff, parents and alumni, established over long periods of time.

7 Trust and Reputation

So much of a school's reputation depends upon the community's trust that the school is always operating with the highest level of professionalism in regard to its online presence.

What would happen to that reputation if exams and results were compromised by a security breach?

Schools recognise the importance of their branding. There is a vast difference in value to the school between an ordinary, anonymous bus, and one driving the streets showcased with the school's name and crest.

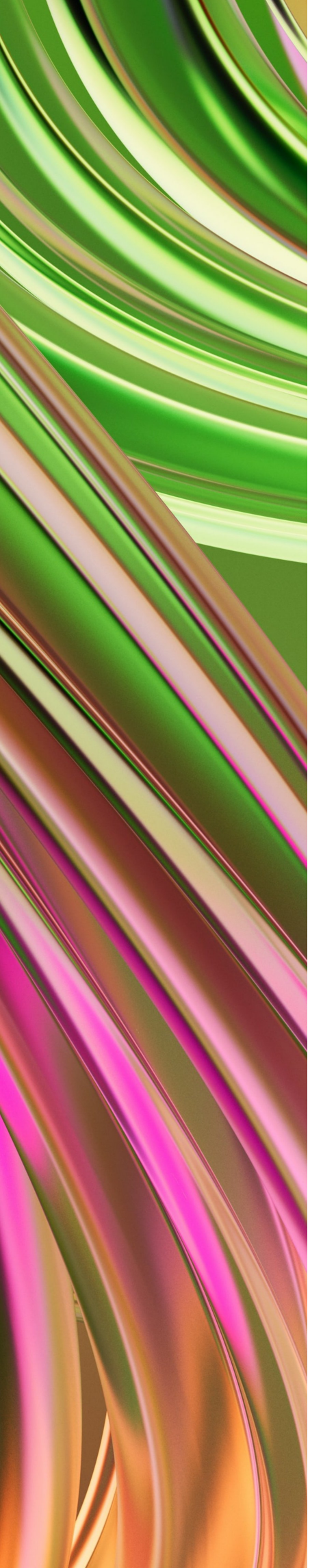
If that identity is hijacked, as happens in phishing attacks, what happens to the school's brand?

Schools have long-term relationships with the communities that depend upon them: the staff, students, parents and alumni. If their private data becomes public then the damage could be enormous.

But what happens if such a breach of personal trust is actually permitted by a school?

In the next section we discuss a school that has allowed a third party, whose interests are not directly aligned with the school, *to use the school's branding for their own purposes* — and the school's reputation has publicly suffered.

Schools must always control their relationships with their own communities.



8 Identity Control

Recently some businesses have sought to use school identity information for marketing promotions, alleged to benefit both the business and the school.

MITIE Inc. is an association of ICT staff in education. A recent MITIE forum pointed out several cases of school community information, email addresses and phone numbers, being released for direct marketing drives, without the permission of the recipients.

One scathing comment was: '*I would suggest that most schools would feel the loss of reputation from what seems like largely unsolicited spam would far outweigh the benefits.*'

Schools must consider issues raised by these questions in terms of protecting their unique identities online:

- What measures have been taken to protect the school's name, brand or identity in the school's online activities?
- Have the identity credentials of people in the school community been transferred to a third party, and if so, how is that documented and protected?
- If the school no longer owns the identities of its community, what control does it have over direct marketing by outside businesses to that community?

If arrangements have been negotiated for any transfer of identity information to non-school entities, always remember the adage: '**If you're not paying for the product, you *are* the product.**' And that applies to your school's hard-won reputation as well.

Any identity compromise is an existential threat to the viability of a school.

9 Integrated Provisioning

The creation, maintenance and continuous protection of identity is a fundamental task facing schools as a whole. But professional identity protection must be built in from the start, and it goes far beyond simple account administration.

Identity protection demands that security is integrated with all aspects of technical provisioning, because identity is the one component that ties all school functionality together.

When considering sources of provisioning, schools must not blindly trust that major vendors, with their own commercial agendas, are always going to do the right thing by their customers.

A recent article by the Federal eSafety Commissioner, *I'm Putting Tech Giants on Notice*,[2] discusses moves to force currently reluctant Big Tech firms, such as Apple, Facebook and Microsoft, to comply with Australian accountability and transparency laws.

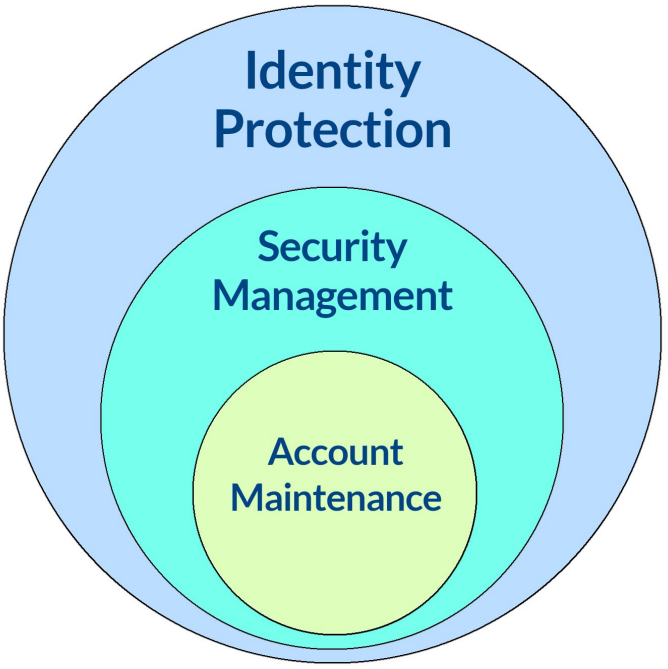
Hence, provisioning must safeguard schools by being *independent* of the limitations of vendors, their technology silos, and their secretive data collection.

Provisioning must adhere to both international technical standards and Australian legal requirements, and must also provide easy, reliable and secure interactions for both administrators and users.

2. https://www.smh.com.au/national/i-m-putting-tech-giants-on-notice-protect-our-kids-20220829-p5bdmx.html

10 Three Spheres of Protection

The safeguarding of schools operates through three *integrated* spheres as shown below: account maintenance, security management, and identity protection.



Studentnet Spheres of Protection

Central Sphere – Account Maintenance

This is the provisioning, propagation and maintenance of accounts and groups from out of a source of truth (the school management system or other sources) into dependent systems such as:

- Directories (AD, Azure AD, Cloudwork)
- Learning management systems (Schoolbox, Canvas, Google Classroom, etc)
- Curriculum systems (Adobe, Clickview, JSTOR, etc)
- Apps (Digistorm, EnrolHQ, etc)
- Portals (EnrolHQ, Elcom, etc)

Middle Sphere — Security Management

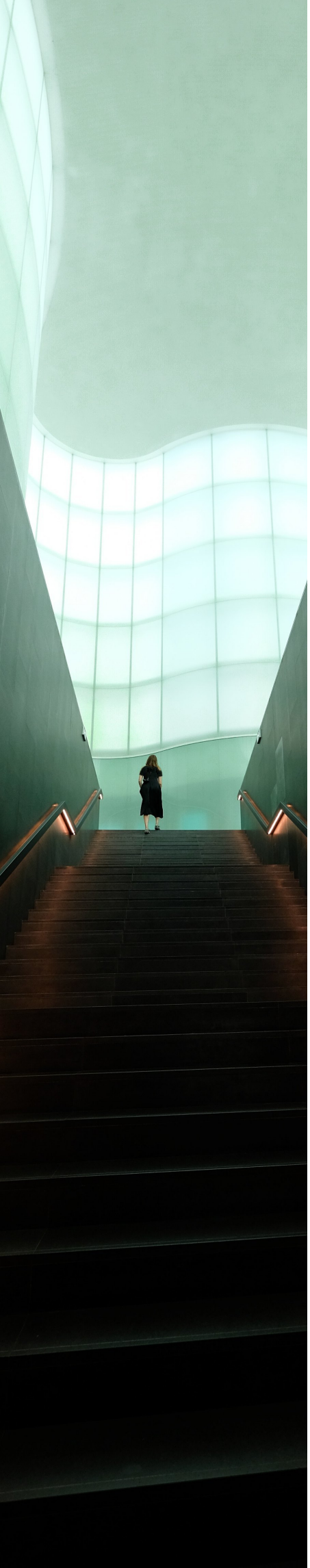
This covers the operation and use of account credentials for the identification, authentication and authorisation of individuals and groups, including:

- Authenticating usernames and passwords
- Multi-Factor Authentication
- Single Sign On
- Password recovery
- User self-management
- Identifying authorised services
- Messaging such as welcomes and broadcasts
- Security policies (password complexity, lockouts, etc)
- Silent Inspection
- Privileged Identity Management
- Protocol support (SAML2, OpenID Connect, FIDO2, InTune, Extensible SSO, etc).

Outer Sphere — Identity Protection

This covers establishing, growing, preserving and maintaining the integrity, authenticity, reliability and validity of the relationship of an identity to the subject being identified. It protects attributes such as:

- **Exclusivity** — ensures that only one entity is the subject of any given identifier, such as in the case of a unique trademark.
- **Reputation** — ensures that an identity is known for its established qualities that contribute to its social or commercial standing.
- **Awareness** — ensures that names and brands are visible both geographically and commercially.
- **Anti-phishing** — ensures that technical connections originate exclusively from the true source.
- **Anti-theft** — ensures that identifiers are protected against identity attacks and misuse.



11 Summary: What is Identity Protection?

Identity protection arises from the measures that protect a school *at every level*, not simply at the information technology stage. Identity protection creates the security boundary of the entire school, from resources, to people, to reputation.

Identity protection of resources must adhere to international technology standards. It must safeguard educational applications by being independent of vendor silos and their limitations. It must be easy, reliable and secure for users and administrators.

Identity protection of people must safeguard the privacy of staff, students, families and alumni, and offer a complete, life-long connection between people and the school. It must allow users to control appropriate aspects of their own digital environment.

Identity protection of reputation must enhance the school's standing, influence and viability, arising from its academic performance, community engagement, and branding in the online world.

Identity protection provides the security perimeter of the entire school, from operational infrastructure, to personal privacy, to institutional reputation.

Studentnet Identity Protection

Studentnet has a long, respected reputation for security at the highest level, and is also uniquely tailored for Australian education requirements.

Studentnet's Cloudwork® provides an *independent* and standards-compliant context for safeguarding schools — Studentnet Identity Protection. It operates through two modalities, SmartID and EasyID:

- **SmartID authenticates identity at the highest security levels**
- **EasyID administers identity across multiple school communities**

SmartID and EasyID provide the functionality required to maintain the security of a school — its infrastructure, its people, and its standing in the world of education.

Studentnet protects identity, and identity protects schools.

Contact Us

Studentnet has been working with schools since 1996. We are dedicated to the needs of educators, students, parents, IT staff and school communities, and are committed to providing the highest possible levels of security and privacy. Please feel free to contact us to discuss this document, security issues, or your school's requirements.

Tel: +612 9281 1626 Email: info@studentnet.net

Address: Suite 1, 89 Jones St, Ultimo NSW Australia 2007

What is Identity Protection?

Schools today face existential threats – identity theft, tech silos and data exploitation:

- How is your school protecting its online reputation?
- Who really owns the identities of your community?
- Does your school exclusively control them?
- Is ownership documented and enforced?

What is your school's strategy for online survival?

Studentnet CLOUDWORK®

Make the cloud yours®