

Global Education Security Standard (GESS) & Privacy Obligation Document (POD)

Steve Smith, Cambridge Public Schools

Connie Coy MOREnet

Jim Siegl, Future of Privacy Forum

Increased interoperability without the inclusion of privacy requirements = increased RISK

CONNECTING

YOUR data management



#1 Global Educational Data Blueprint

FIND OUT MORE >>

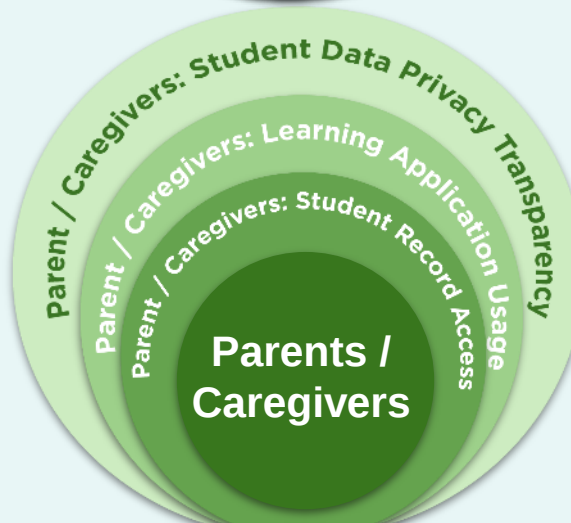
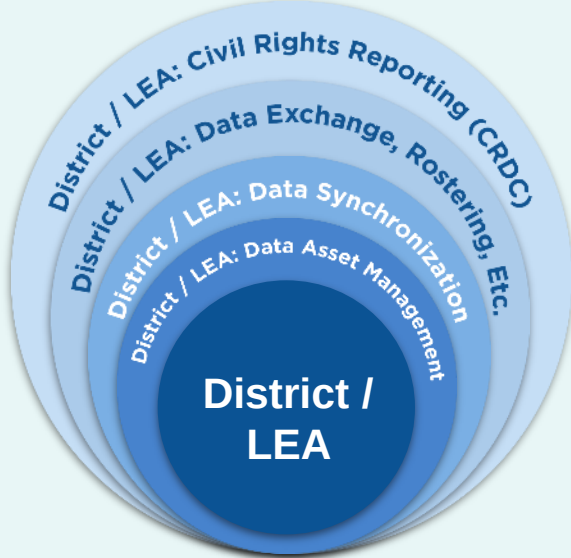
SECURING

YOUR data privacy



Tactical Student Data Privacy Support

FIND OUT MORE >>



What's needed
is a **connected,**
secure, and
effective learning
ecosystem

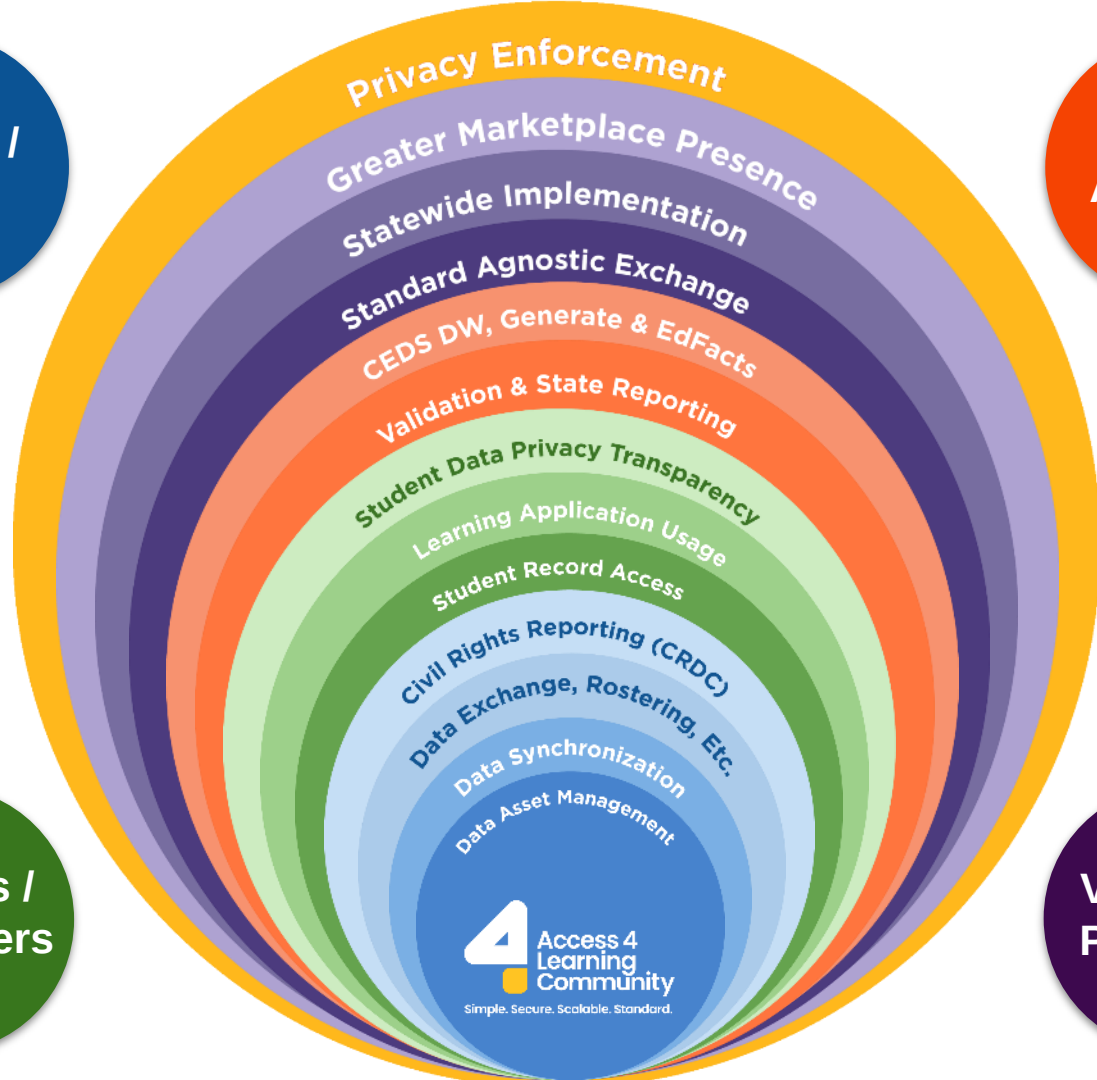


District /
LEA

State
Agencies

Parents /
Caregivers

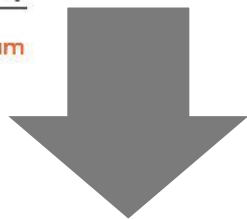
Vendors /
Providers



Connected
and Secure
Effective
Learning
Ecosystem
TM



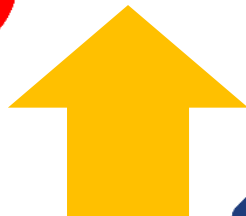
It's Not "One or the Other"!



***No One
Gets It!***

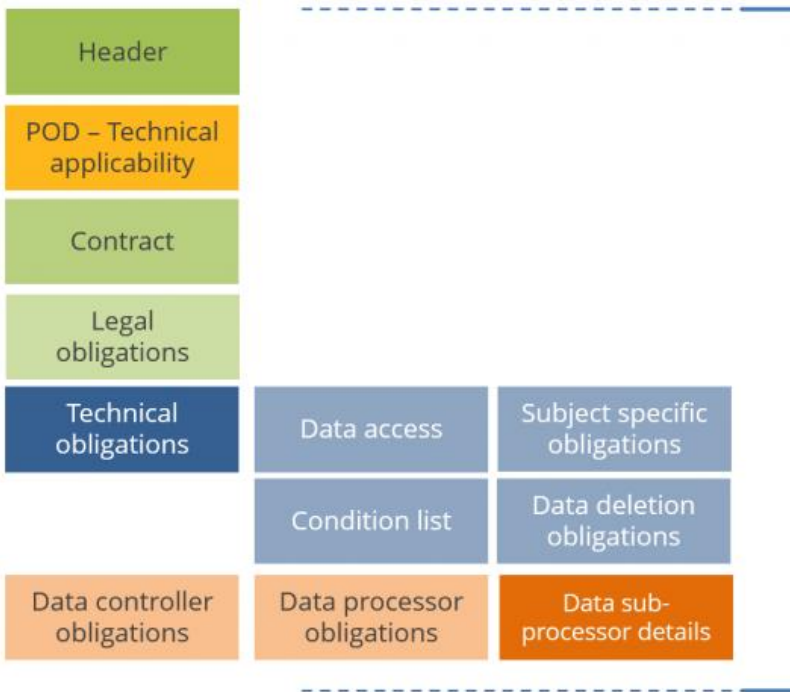


***Everyone
Gets It!***



***“Connecting and
Securing Effective
Learning Ecosystems”®***

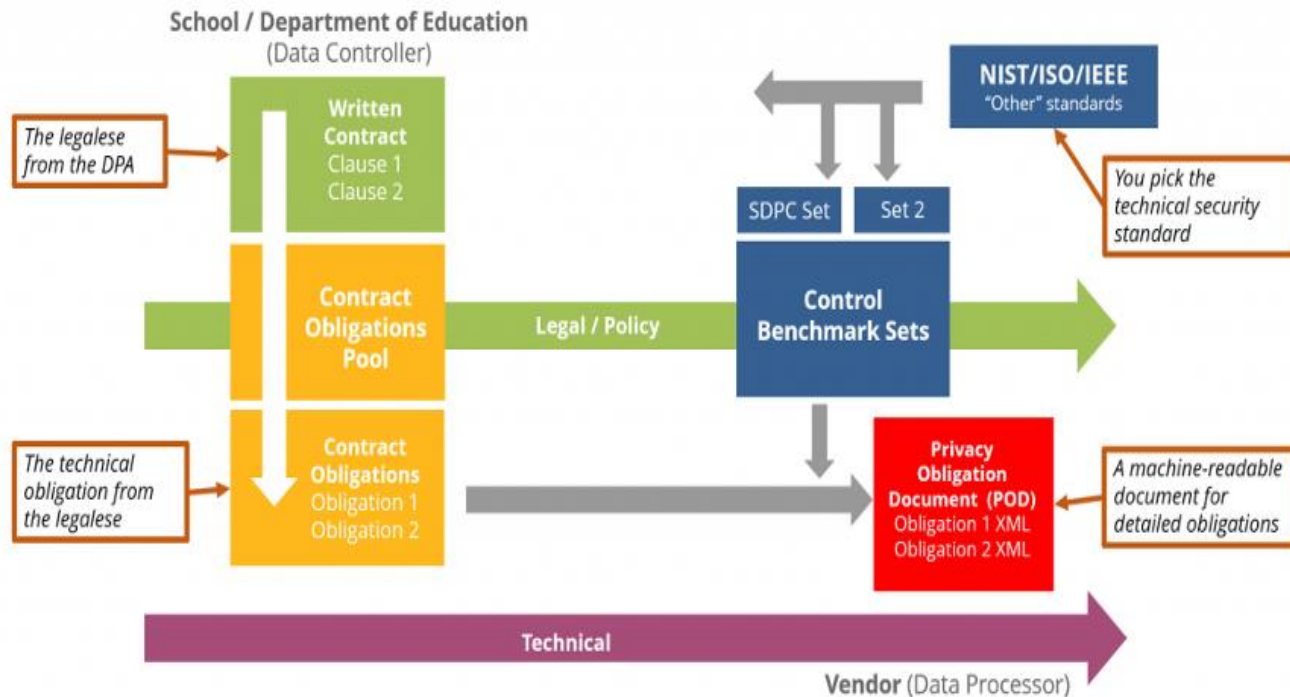
Privacy Obligation Document



**Automate Contract
Clause Expectations
Exchange and Vendor
Verification**

The “POD”
(Privacy Obligation Document)

End-to-End Privacy Solution?

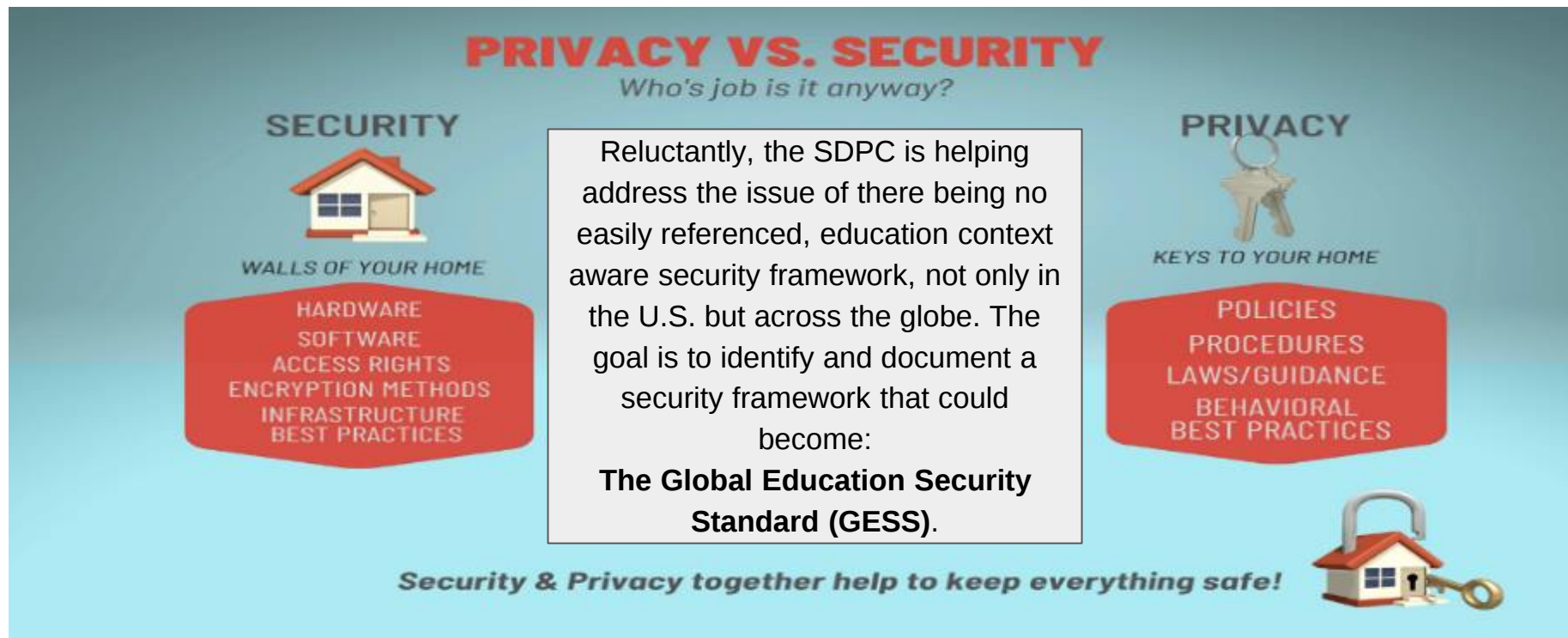


Automate Contract Clause Expectations Exchange and Vendor Verification

The "POD" (Privacy Obligation Document)



Global Education Security Standard



Graphic from CITE: studentdataprivacy.net

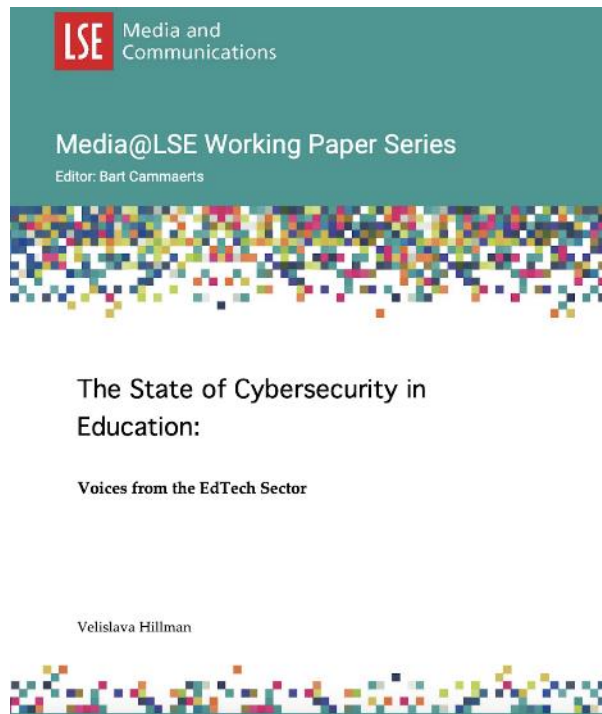
Security Requirements to Meet Privacy Obligations

- No standard Requirement
- “Industry Standards”
- “Best Practices”
- Some Jurisdictions have mandated control sets; NH, NY, IL, TX AU NZ
- Most do not
- Everyone is struggling consumers & providers

- Lack of providers understanding K-20 cybersecurity educational needs/concerns
- Provider's policies are not written to address district concerns.
- Provider Contract/District Agreements
- Free apps/free version
- Remove negativity from negotiations
- Reputable standard framework



An ideal cybersecurity
standard must
**underpin children's
safety and data
privacy and address
the challenges** of the
entire EdTech sector



CONNECT
Velislava Hillman (PhD)
[veli@edds-
education.org](mailto:veli@edds-education.org)
EDDS @ ETOILE
PARTNERS



EDDS



etoile

Where to start...

Where to start on a Global Education Security Standard?

- ST4S Introduction
- Leverage the work of ST4S
- Mapping ST4S and all relevant frameworks
- Identify specific controls across frameworks
- Format & publish new set of controls

What is ST4S?

An assessment framework for digital products and services used in the Australian & New Zealand Education Sectors against agreed criteria for:

- Security
- Privacy
- Functionality / Online Safety
- Interoperability

Started with Australian States and Territories only, expanded recently to include New Zealand.

Safer Technologies 4 Schools Assessment

Sample product/service (Sample vendor)

Assessment outcome: Medium risk

A non-compliant assessment outcome means the service does not meet the minimum requirements for information security, privacy, and/or online safety.



Service summary

Version:	Paid – Latest	Review date:	18/05/2020
Tags:	Library management; Administrative support services; Booking systems.	Assessment Tier:	Tier 2
URL:	http://www.sampleproduct.com.au	Audience:	Staff and Students
Purpose of use:	Sample product is a library management system. Modules include cataloguing, circulation, search, overdue notices, borrowers, reports and stocktake.		

Information assets and hosting

Data hosting: Service components Onshore (in Australia) **Data classification:** ☒ Non-personally identifiable information

- Engaged with over 400 products/services
- Genuine, detailed assessments are hard and take time
- Just over 50% completion rate
- Most suppliers want to do the right thing
- Majority of suppliers make changes to improve their offerings

All suppliers appreciative of consistent approach with shared results

Global Education Security Standard

Establish a consolidated approach:

- Leverage shared efforts and success of SDPC (USA)

- Leverage assessment approach and success of ST4S (AU/NZ)

Geared to online products / services

Considers a number of existing frameworks:

- NIST 800-171 & 800-53

- CIS – Critical Security Controls v8

- UK Cyber Essentials (July 2022)

- AU ISM, NZ ISM

Draft set developed of control statements with assessment questions and possible answers

Global Education Security Standard (GESS)

Identify and document a security framework that could be a global security blueprint leveraging the ST4S work in the AU.

[Presentation shared with you: TSI x](#)
[SDPC Community Update Aug 2 x](#)
[Mappings - Google Drive x](#)
[NIST 800-171 Matrix - Google Slides x](#)

[docs.google.com/spreadsheets/d/16oQTo6S5aivgr-wjMorTkU3RkewB4sZkPNdSuR5Sa0/edit#gid=0](#)

NIST 800-171 Matrix

File Edit View Insert Format Data Tools Extensions Help [Last edit was made 14 days ago by Martin Rothbaum](#)

100% 11

A3-Are vendor staff, external contractors or associates with

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	NIST 800-171 Control	Control Type	Control Text		NIST 800-53	ST4S detail	UK Cyber Essentials	Valid in education SaaS context?	Applicability Scope	Suitability Notes/Use Cases											
2	3.1.1	Basic	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).		AC-2, AC-3, AC-5	AS - Does your organisation provide access to systems based on roles (e.g., role-based access control (RBAC)), and is this process documented for all systems including the service?	User access control	Essential	Product												
3	3.1.2	Derived	Limit system access to the types of transactions and functions that authorized users are permitted to execute.		AC-2, AC-3, AC-5	AS - Does your organisation provide access to systems based on roles (e.g., role-based access control (RBAC)), and is this process documented for all systems including the service?	User access control	Essential	Product												
4	3.1.3	Derived	Control the flow of CUI in accordance with approved authorizations.		AC-4			Essential	Product	Will result in multiple controls being facing (firewalls and other bound packet inspection etc)											
5	3.1.4	Derived	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.		AC-5			Essential	Both	Will require controls for the prod administrators vs end users and there separate testing teams vs d											
6	3.1.5	Derived	Employ the principle of least privilege, including for specific security functions and privileged accounts.		AC-6, AC-6(1), AC-6(2)	What is the service's approach to default user access permissions (e.g., all access is denied unless specifically allowed, all access is allowed unless specifically denied)?	User access control	Essential	Product												
7	3.1.6	Derived	Use non-privileged accounts or roles when accessing nonsecurity functions.		AC-6(2)		User access control	Optional	Product	If product supports role based advice regarding product configu											
8	3.1.7	Derived	Prevent non-privileged users from executing privileged functions and audit the execution of such functions in audit logs.		AC-6(9), AC-6(10)	AS-Are vendor staff, external contractors or associates with non-privileged accounts restricted from installing, uninstalling, disabling or making any changes to software and system configuration on servers and endpoints? L1- Does your organisation have a documented and implemented logging procedure which requires all systems in your organisation (e.g., servers, storage, network, applications, etc.) to log the following and synchronise logs to a consistent time source:	User access control	Essential	Product	Requires at least 2 controls: RBAC logs											

3.1 Access Control 3.2 Awareness Training 3.3 Audit & Accountability 3.4 Configuration Management 3.5 Identification & Authentication 3.6

Count: 2 [Explore](#)

Multi-factor authentication

NIST 800-171: 3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

CIS 6.4: Require MFA for remote network access.

CIS 6.5: Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

AU ISM 1173: Multi-factor authentication is used to authenticate privileged users of systems.

NZ ISM 16.7: To ensure authentication systems incorporate Multi-Factor Authentication mechanisms to secure Privileged Accounts and in accordance with the Agency's Privileged Access Management (PAM) policy.

UK A7.14 Have you enabled multi-factor authentication (MFA) on all of your cloud services?

UK A7.16 Has MFA been applied to all administrators of your cloud services?

Multi-factor authentication

Question format: Does your organisation mandate multi-factor authentication for:

Vendor staff, external contractors or associates accessing systems remotely (including access to cloud systems);

System administrators;

Support staff;

Staff with privileged accounts?

Control statement format: Multi-factor authentication is mandated for:

Vendor staff, external contractors or associates accessing systems remotely (including access to cloud systems);

System administrators;

Support staff; and

Staff with privileged accounts

The screenshot shows a web browser window displaying the GESS Portal. The browser's address bar shows the URL `sdpcall.org/gess_home.php`. The website has a blue header with the Access 4 Learning Community logo and navigation links: "About the Consortium", "Join the Community", "Resource Center", "News and Events", and "Login". Below the header is a green banner with the text "Global Education Security Standard (GESS)".

The main content area features a paragraph: "Global Education Security Standard (GESS) is a matrix/crosswalk of all existing security frameworks along with the core set of controls applicable to PK-20 data." Below this is a section titled "About GESS" with a bulleted list:

- GESS is an internationally agreed upon set of security controls pulled from major cyber security frameworks that are most applicable to the PK20 education ecosystem.
- By joining the GESS subscribers you will be aiding the movement of the EdTech industry towards one common set of security controls to apply across many jurisdictions, thus avoiding the need to prove certification in multiple frameworks PK20 schools and districts are adopting the GESS set of controls as the expected security measures to be in place to protect all student data.
- In the US the next version of the National Data Privacy Agreement will include the GESS as an approved and accepted control framework In New Australia & New Zealand the preexisting ST4S controls are embedded within GESS.
- GESS will streamline both the providers' ability to implement required security controls while at the same time meeting school expectations all with one common set of controls.

Below the list is a button labeled "Learn more >>".

The bottom section of the page contains three white cards with orange icons and text:

- GESS Documentation**: View a comprehensive report on control questions and response options for K-12 EdTech. Includes a "Download the File" button.
- GESS Self Assessment**: How do your score? Find out by using the GESS Self Assessment Tool. Includes a "Begin Assessment" button.
- Other Ways to Explore GESS**: This is a longer card with supporting text below as a natural lead-in to additional content. Includes a "Start Exploring" button.

GESS V1.0 RELEASED YESTERDAY!