

Smith Coins: client-held progress tokens for data-minimised learning on the web

Syed Zaidi · Lessonsmith Ltd, London, UK · lessonsmith.net

ORCID: <https://orcid.org/0009-0004-0800-1646> · Preprint · 24 October 2026

Abstract

Smith Coins let pupils keep and resume their progress on a learning website without an account, a name, an email address or any server-side record of who they are. Each coin is a short check-summed code (for example SMITH-XXX-XXX-XXX) or a downloadable PNG "coin picture" whose metadata carries the saved work. The pupil holds it, and the server never needs to identify them.

This paper describes the concept, places it against research on privacy by design, data minimisation and client-held credentials, and reviews related patents. It then reports a working implementation in the Lessonsmith platform. There are four pupil coding tools (Turtle Range, Python Playground, Code Detective and AI Labs), and an invitation-only SEND Suite in which trial coins open encrypted records that become unreadable when the trial key is deleted.

The implementation runs in production and is covered by an automated test suite. We argue that client-held progress tokens are a practical way for schools and edtech providers to meet the data minimisation principle of UK GDPR and the ICO Age Appropriate Design Code. We also set out the limits: lost coins, shared devices, the absence of cross-device sync, and the fact that a coin is a bearer token.

Keywords: data minimisation; privacy by design; children's data; education technology; client-side storage; bearer tokens; gamification; crypto-shredding; SEND

1. Introduction

Most learning websites ask a pupil to sign in before they can save anything, so a name, an email address or a school login becomes the price of keeping progress. That record then has to be secured, justified, retained and eventually deleted, and it can leak.

The risk is not hypothetical. Human Rights Watch's May 2022 report "*How Dare They Peep into My Private Life?*" examined 164 education technology products endorsed by 49 governments. It found that 146 of them (89%) appeared to use data practices that put children's rights at risk, many sending children's data to advertising technology companies [8].

In the UK, Article 5(1)(c) of the UK GDPR requires personal data to be "adequate, relevant and limited to what is necessary" [10, 15]. The ICO's Age Appropriate Design Code, which online services likely to be used by children have had to conform to since 2 September 2021, makes data minimisation one of its 15 standards (standard 8) and covers educational websites explicitly [9]. The Data (Use and Access) Act 2025 goes further. Section 81 adds Article 25(1A) to the UK GDPR, which requires services likely to be used by children to weigh "children's higher protection matters" when designing their data protection measures [5].

The research question is therefore practical: **can a learning service give pupils durable, resumable, rewarded progress while collecting no personal data about them at all?** We answer it with a design, Smith Coins, and a working test of that design across five tools in the Lessonsmith platform. The contributions are:

1. A model of progress as a pupil-held bearer token rather than a server-side account.
2. Two encodings of that token: a short check-summed code a pupil can copy by hand, and a coin picture (PNG) that carries a full save inside its metadata.
3. A variant for sensitive adult use (SEND records) in which records are encrypted with a trial key held by the server and destroyed at the end of the trial, so the records on every coin become unreadable at once.
4. A report of the implementation, its automated tests and a mapping against UK data protection requirements.

2. Background and related work

Smith Coins combine five existing ideas: privacy by design, identity-free transactions, password saves from video games, data carried inside images, and erasure by key destruction. None of the work reviewed applies all five to school pupils' learning progress.

Privacy by design and data minimisation. Cavoukian's seven foundational principles include privacy as the default setting and full functionality as "positive-sum, not zero-sum" [3]; data protection authorities endorsed the approach by resolution in 2010. In learning analytics, Drachsler and Greller's DELICATE checklist addresses how institutions can use learner data in a trusted way [6]. Smith Coins take the stricter position of not identifying the learner at all.

Security without identification. Chaum argued that transaction systems can protect individuals by letting them act through credentials that do not reveal identity [4]. The W3C Verifiable Credentials Data Model 2.0, a W3C Recommendation since May 2025, builds signed, holder-kept credentials on that idea [16]. These systems prove claims about a known subject; a Smith Coin proves nothing about a person and only restores work.

Capability URLs and bearer tokens. The W3C TAG's guidance on capability URLs describes links that grant access to whoever holds them, removing the need for logins, and warns that such links can leak [14]. A Smith Coin code is a capability of the same kind and inherits the same leak risk (section 6).

Password saves. Home video games used typed passwords to restore progress from 1983 onwards; Metroid's 1987 US release encoded items, doors and bosses into a long password of letters and numbers because the console could not save to disk [17]. Smith Coin codes follow this tradition but add a check value and a scramble, so that typing slips are caught and codes are hard to guess.

Data inside images. The Open Badges baking specification embeds a badge assertion in the badge's own PNG or SVG image so that software can extract and verify it [2]; Open Badges 3.0 (2024) moves trust to signed verifiable credentials [1]. Smith Coin pictures use a similar mechanism, a PNG metadata chunk, but to carry the save itself rather than a claim about a named earner.

Local-first software. Kleppmann et al. argue that users should own their data on their own devices rather than in the cloud [11]. Smith Coins are local-first in this sense, without the sync layer.

Crypto-shredding. Encrypting data under a key and destroying the key renders every copy unreadable, including copies that cannot be found [13]. Vendors note that this does not by itself guarantee legal erasure [12]. The SEND Suite variant applies it to records the server never holds.

Gamification. Hamari, Koivisto and Sarsa's review of 24 empirical studies found mostly positive effects of points and badges, dependent on context and users [7]. Smith Coins use quarters, tiers and XP as rewards, so this evidence and its caveats apply.

3. Patent and prior-art review

The search found patents for each building block on its own, but none that covers a pupil-held progress token, in code or image form, used instead of an account in an education service. Table 1 lists the closest documents found in Google Patents and USPTO records.

Document	Title (owner)	What it covers	How Smith Coins differ
US 11,100,754 B2; US 2021/0383646 A1	Method of enabling restoration of games and a method of restoring games (Aristocrat Technologies Australia; priority 2009)	Restoring a gaming-machine session from a game state identifier on a ticket or typed in, checked against a server session identifier	No server session or player record; the coin itself is the save
US 6,923,721 B2	Apparatus and method for maintaining game state (Sierra Design Group; now LNW Gaming; lapsed for unpaid fees)	Keeping a player's game state on a portable device to resume later	A typed code or an ordinary image file, not a device
US 8,365,081 B1	Embedding metadata within content (Amazon Technologies, filed 2009)	Metadata in a media file, including instructions for the receiving application	Coin pictures carry learning progress for one web tool, restored only when the pupil uploads them
US 8,949,610 B2	Method for embedding secret message into PNG image (National Chiao Tung University, granted 2015; lapsed for unpaid fees)	Hiding a message in a PNG's alpha channel (steganography)	A visible, standard PNG text chunk, not hidden pixels
US 8,984,650; 9,542,573; 9,807,061	Privacy server for protecting personally identifiable information (Pearson Education, priority 2012)	A privacy server that replaces a student's identifier with a token so that a learning management system can track progress	The personal data still exists behind the token; Smith Coins never collect it
US 2012/0093318 A1	Encryption key destruction for secure data erasure (SandForce / LSI; granted as US 8,938,624 B2)	Erasing a storage device by destroying its key material	A trial key on a server is destroyed to make records held in users' own coin pictures unreadable
US 2013/0305057 A1	Cryptographic erasure of selected encrypted data (IBM, filed 2012; granted as US 8,918,651 B2)	Per-file key destruction on tape storage	As above: the records are off the server, in files the users keep
Open Badges baking (open standard)	Badge baking (IMS Global, 2018)	An achievement assertion embedded in the badge image	A badge names an earner; a Smith Coin restores work and names no one

Table 1. Closest patents and standards. The claims were not analysed in full and legal status was taken from public records; this is a prior-art survey, not a freedom-to-operate opinion or a patentability search.

4. The Smith Coins design

A Smith Coin is the pupil's progress, written down in a form the pupil can carry away. The service keeps the work in the browser tab for the current visit only, and on leaving the pupil takes a coin. On the next visit, on any device, the coin restores the work (Figure 1).

The pupil carries the coin; the server never sees it

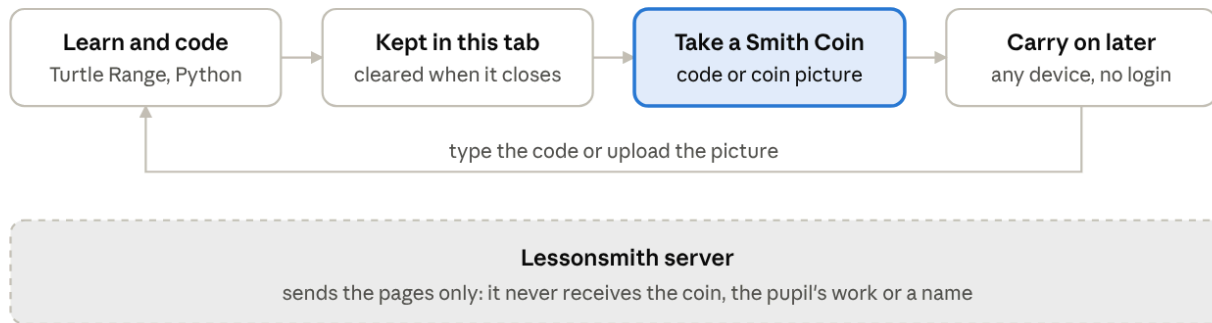


Figure 1. Smith Coin lifecycle in the pupil tools. The loop closes through the pupil, not the server: progress leaves the browser only as a coin in the pupil's hands.

4.1 Four forms of coin

Form	Example	What it holds	Where it is checked
Short code (Experiments)	SMITH-XXX-XXX-XXX (9 characters)	Missions done, which were done in Python, current mission, block or Python mode, and XP (35 bits), plus a 10-bit check	In the browser; nothing is sent
Short code (AI Labs)	SMITH-XXX-XXX-XXX-XXX (12 characters)	For each of 3 labs: steps done, best challenge, XP in tens; and the year group (49 bits), plus a 10-bit check	In the browser; nothing is sent
Coin picture	A PNG of the coin	Everything in the code, plus the pupil's typed programs and Code Detective work, in a PNG text chunk	In the browser, when the pupil uploads it
Trial coin (SEND Suite)	SMITH-RD-XXXX-XXXX-XXXX	A random 60-bit code; the server keeps only its SHA-256 hash	On the server, which returns the trial key while the trial is live

4.2 How a code is built

Progress is packed into an integer, field by field, with a version number at the top. The integer is scrambled by a reversible function (multiplication by an odd constant modulo 2^{35} , then an xor-shift), so that neighbouring progress gives unrelated-looking codes. A 10-bit check value computed from the unscrambled integer is appended, and the result is written in Crockford-style base 32, which leaves out I, L, O and U so that pupils cannot confuse them with 1 and 0.

On entry, the code is normalised (spaces, dashes, case and look-alike letters), unscrambled and checked. A mistyped code fails the check about 1023 times in 1024, so a typing slip is caught rather than restoring the wrong progress.

4.3 Coin picture

The coin picture is an ordinary PNG drawn on a canvas, showing the coin, its tier, the facts it records and its code. The full save (a small JSON object) is stored in a PNG tEXt chunk with a fixed keyword and its CRC32 recomputed, much as Open Badges baking embeds a badge assertion. Image viewers ignore the chunk; the Lessonsmith page reads it back when the pupil uploads the picture.

4.4 Rewards without records

Coins grow in quarters, halves and wholes as missions are completed. The coin's metal shows how many cases are solved: Lessonsmith green to start, Bronze for one case, Silver for two, Gold for three, and Platinum for every mission done in text-based Python. Stars repeat the tier, so colour is never the only cue. XP is earned for missions (+10), for Python (+5) and for solving a case (+20); a hint costs 5 XP or a free 30-second wait. All of this is computed from the coin, so no leaderboard or server-side profile is needed.

4.5 Leaving and shared computers

Work is kept in `sessionStorage`, which the browser clears when the tab closes, so a pupil on a shared school computer cannot pick up the previous pupil's work. When a pupil tries to leave the coding section with unsaved progress, the page offers the code and the coin picture first.

4.6 The SEND Suite variant: records that expire

The SEND Suite holds sensitive adult records (precision-teaching timings, timetables and cover plans), so its coins work differently.

1. A school requests a trial (1 to 32 staff, 1 to 8 weeks) and receives a reference and a private pickup key. It verifies itself by emailing a staff ID card, which is deleted after checking.
2. The owner authorises the trial, and the server creates a random 256-bit trial key.
3. The school collects one coin per member of staff with its reference and pickup key. The codes are shown once; the server keeps only their hashes.
4. Opening the Suite with a live coin returns the trial key. Records are encrypted in the browser with AES-GCM and saved inside the staff member's coin picture, never on the server.
5. When the trial ends, the server deletes the key and the coin hashes. Every copy of every record, wherever it is stored, can no longer be opened. Contact details are deleted 30 days later.

5. Implementation in Lessonsmith

Smith Coins run in five tools on lessonsmith.net, built with Node 22, Express 5 and plain browser JavaScript. The pupil tools need no login, and Python runs in the browser through Pyodide, so pupils' code is not sent to the server either.

Tool	Who uses it	Coin	Server involvement
Turtle Range	Pupils: 14 turtle missions in 3 cases (Hatchling, Explorer, Ranger), in Lessonsmith blocks or Python	9-character code, coin picture	Serves the page only
Python Playground	Pupils: free Python practice	Coin picture (holds the typed program)	Serves the page only
Code Detective	Pupils: debugging cases	Coin picture (holds case work)	Serves the page; optional AI hints
AI Labs	Pupils in a teacher-run session: 3 labs of 7 steps each	12-character code, coin picture	During a live session only: a random nickname (an adjective and an animal), the step reached and quiz scores, deleted with the session; no pupil names
SEND Suite (R&D)	School staff on an approved trial	Trial coin: code plus encrypted coin picture	Trial records, coin hashes and the trial key; never the pupil records

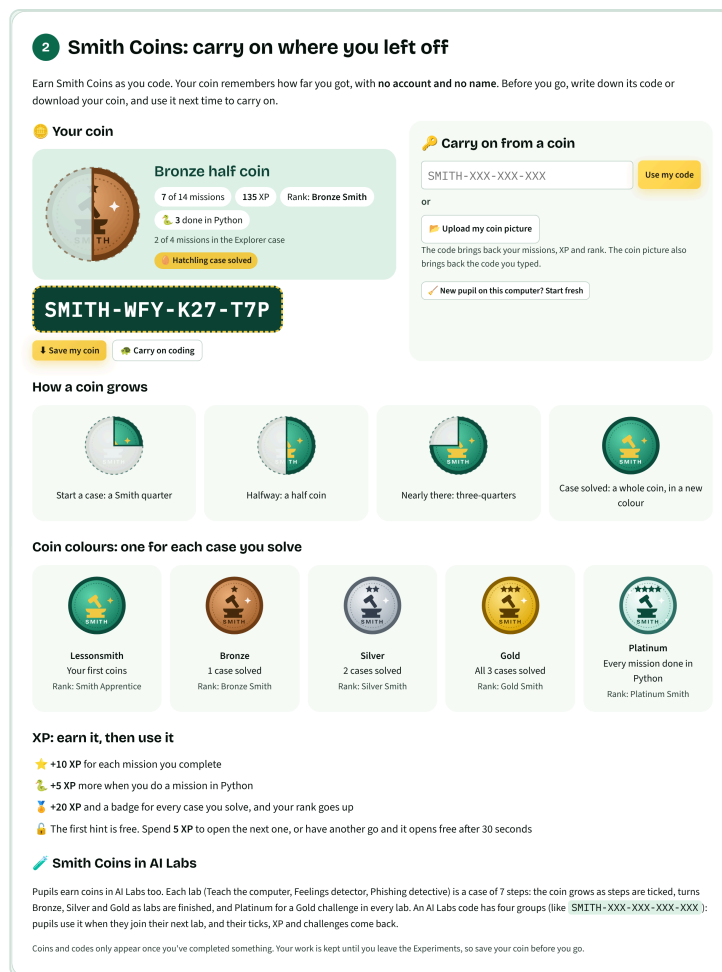


Figure 2. The Experiments page restores a pupil's progress from a code alone. The test code SMITH-WFY-K27-T7P brings back 7 of 14 missions, 3 in Python, 135 XP and a Bronze half coin.

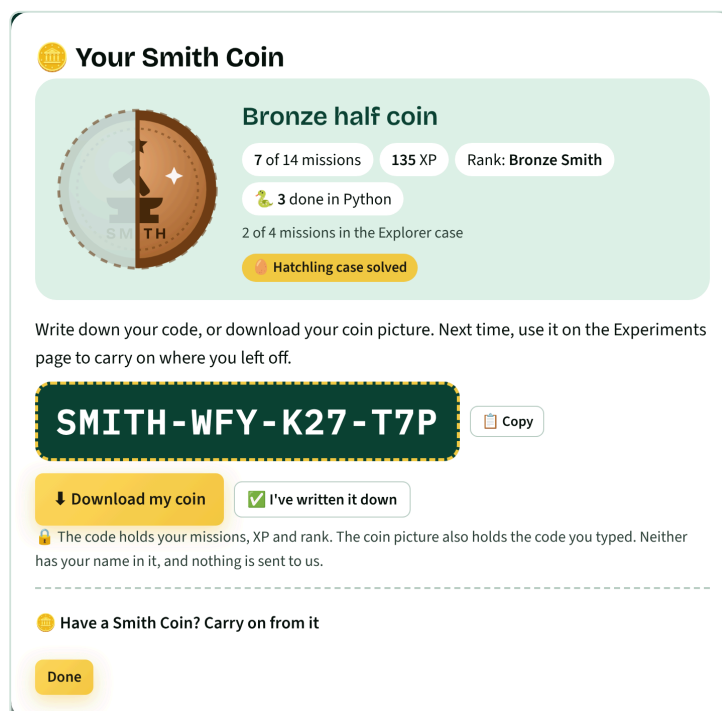


Figure 3. Before leaving, the pupil is offered the code and the coin picture. The notice reads: "Neither has your name in it, and nothing is sent to us."

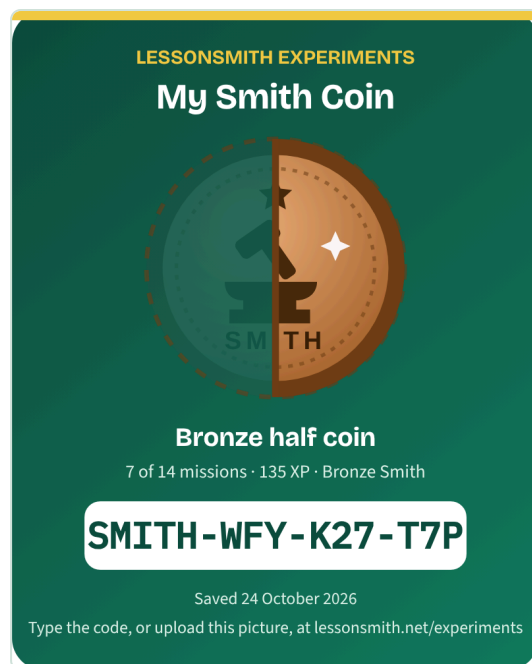


Figure 4. The coin picture is a normal PNG that pupils can keep or print. The full save is stored inside it, in a PNG text chunk.

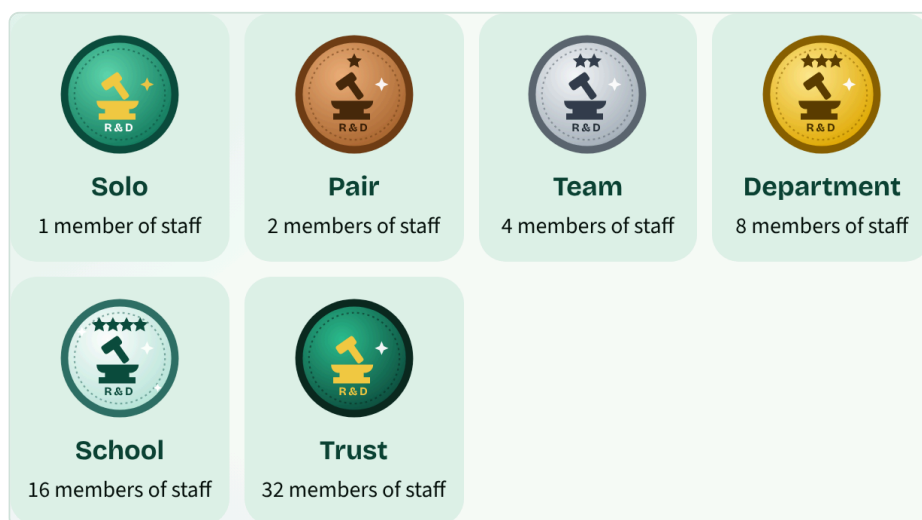


Figure 5. SEND Suite trial coins reuse the Smith Coin design. Their type shows the trial size, from Solo (1 member of staff) to Trust (32).

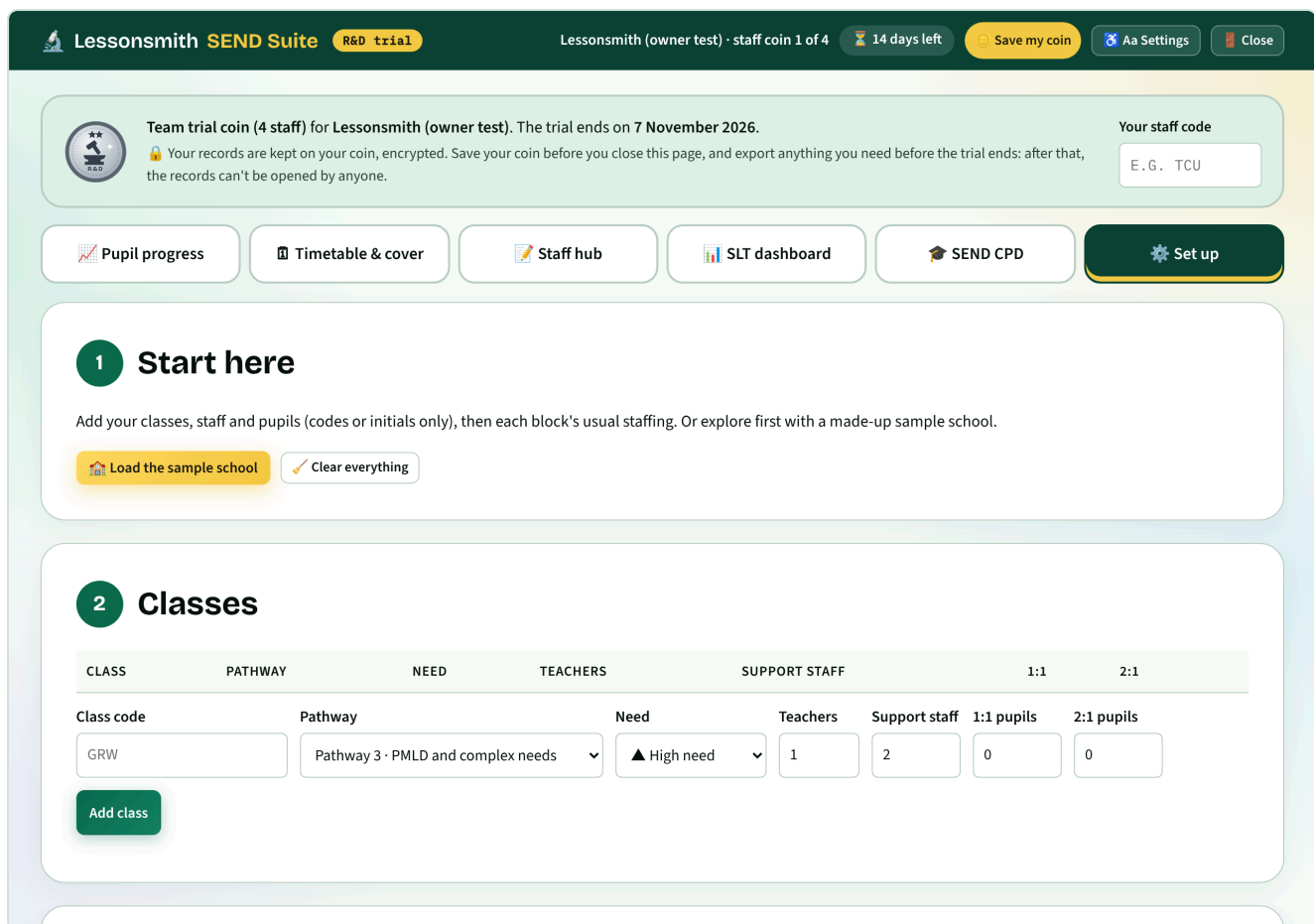


Figure 6. The SEND Suite opened with a test trial coin. The banner explains that records are kept on the coin, encrypted, and cannot be opened by anyone after the trial ends. Pupils are entered as codes or initials only.

All figures are screenshots of the real tools running locally from the production code on 24 October 2026. The SEND Suite screenshot uses the owner's test trial, not a school.

6. Evaluation as a working test

The concept works as built. On 24 October 2026 all 115 automated tests in the Lessonsmith suite passed, including 20 that test the Smith Coin and SEND Suite coin behaviour directly and 3 that check pages make no third-party requests on load. A browser check restored a pupil's full progress from a 9-character code and downloaded the coin picture. None of the page's requests carried progress, a code or any identifier. The check also found that pages loaded Google Fonts; the fonts were then moved to Lessonsmith's own server, so a page now makes no third-party requests (section 7).

6.1 Automated tests

Test file	Tests	What is shown
smith-coins.test.js	9	Coins grow from quarters to whole and change tier per case solved; a code restores missions, Python marks, XP, place and mode; over 99% of single-character typos are rejected; the coin picture carries the whole save; an edited coin file can only restore valid progress; AI Labs codes and pictures round-trip
rd.test.js	6	A trial request is validated and only a hash of the pickup key is kept; coins can be collected only after authorisation, and only once; a coin returns the trial key only while the trial is live; reissued coins replace old ones; at expiry the key and coin hashes are deleted, then contact details 30 days later

Test file	Tests	What is shown
rd-core.test.js	5	Records on a coin open only with that trial's key; colleagues' coins merge without duplicating records; the CSV export is safe against spreadsheet formula injection
third-party.test.js	3	No page loads Google Fonts; every self-hosted font and its licence is present; no page loads an external video player before the visitor presses play

6.2 What reaches the server

Tool	Sent to the server	Personal data kept
Turtle Range, Python Playground	Page requests only	None
Code Detective	Page requests; for an AI hint (signed-in teacher accounts only), the question and code are passed to the AI model	None; only token counts are logged against the teacher's account
AI Labs	Live-session progress under a random nickname	None after the session
SEND Suite	The request form (name, role, organisation, work email); a coin code when opening	Contact details until 30 days after the trial; pupil records never

6.3 Mapping to UK data protection principles

Requirement	How Smith Coins address it
Data minimisation, UK GDPR Art. 5(1)(c); Children's Code standard 8	No pupil identity is collected; progress lives with the pupil
Storage limitation, Art. 5(1)(e)	Pupil work lasts for the browser visit; SEND trial keys and coin hashes are deleted at expiry, and contact details 30 days later
Integrity and confidentiality, Art. 5(1)(f)	SEND records are encrypted with AES-GCM in the browser; codes are stored only as SHA-256 hashes
Data protection by design and default, Art. 25, including the children's higher protection matters in Art. 25(1A)	Saving without an account is the default, not an option
Shared devices	sessionStorage clears when the tab closes, so the next pupil starts fresh

This mapping is the author's analysis, not legal advice or a regulator's view.

6.4 Threat model

Threat	Effect	Mitigation and residual risk
A coin code is seen or shared	Someone else can continue that pupil's progress	Low impact: the coin names no one. Pupil coins are not access controls
A pupil forges a higher coin	False progress	The check value is not a cryptographic signature and the logic is in the browser, so a determined pupil could forge a coin. Acceptable for practice; not acceptable if coins earn prizes (section 7)
A coin picture is edited	Invalid or inflated save	The save is cleaned on upload, so only valid progress is restored
A trial coin leaks during a trial	Someone can open that member of staff's coin picture, if they also have the file	The owner can reissue coins; old codes stop working at once
The server is breached during a trial	Trial keys are exposed	Records are not on the server, so an attacker also needs the staff's coin pictures

Threat	Effect	Mitigation and residual risk
A coin picture is copied after a trial	None	The key is deleted, so the records cannot be decrypted

7. Discussion and limitations

Smith Coins move the job of remembering from the service to the pupil. This removes the privacy risk, but it also moves some costs onto pupils and teachers.

- **Lost coins mean lost progress.** There is no account to recover. A short code is easy to write in an exercise book, but a pupil who loses both the code and the picture starts again.
- **Teachers see only what pupils show them.** No dashboard of pupil progress is possible without collecting data. A teacher can ask pupils to show their coin, which keeps the pupil in control.
- **Coins are bearer tokens and can be forged.** Anyone holding a code can use it, and the check value catches typing mistakes but is not a signature. This is acceptable for practice. It is not acceptable if coins earn prizes such as gift vouchers: prize claims would need a server-side check of the work, or signed coins issued by the server, which would bring back some data processing.
- **Third-party requests.** The browser check found that pages loaded Google Fonts, which told Google the visitor's IP address. The fonts are now served from Lessonsmith's own server, and videos (Synthesia) load only when a visitor presses play, so opening a page makes no third-party request.
- **Crypto-shredding is not settled law.** Deleting the trial key makes SEND records unreadable, but whether that counts as erasure under UK GDPR is the controller's assessment, not a guarantee.
- **No study with pupils yet.** This paper shows that the design works technically. It does not yet measure whether pupils keep their coins, whether codes are copied correctly at different ages, or whether the rewards change motivation. The evidence on gamification suggests the effect will depend on context [7].
- **Author bias.** The design, implementation and evaluation are by the same author. Independent review and replication are welcome.

8. Conclusion and future work

A learning service can give pupils durable, resumable and rewarded progress without collecting any personal data about them. Smith Coins do this by turning progress into a token the pupil holds: a short check-summed code or a coin picture with the save inside. The SEND Suite variant extends the idea to sensitive records, which are kept encrypted on staff's own coins and become unreadable when the trial key is deleted.

The design is running in five Lessonsmith tools and passes its automated tests. Next steps:

1. A classroom study across Key Stages 2 and 3, measuring coin retention, code-copying errors and engagement.
2. Server-signed coins for any use where coins carry value, such as prizes.
3. An automated check, run on every release, that pages make no third-party requests.
4. An open specification of the code and coin picture formats, so that other services can adopt them.
5. Independent legal review of the crypto-shredding approach for SEND records.

Availability. The tools can be tried at lessonsmith.net/experiments without an account. The SEND Suite is available by invitation through the Partner page.

Competing interests. The author develops and operates Lessonsmith (Lessonsmith Ltd).

References

1. 1EdTech (2024). Open Badges 3.0 standard released. Press release, 29 May 2024. 1edtech.org
2. IMS Global Learning Consortium (2018). *Open Badges Baking Specification*. IMS Final Release, 12 April 2018. <https://w3id.org/openbadges/baking/>
3. Cavoukian, A. (2009, revised 2011). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.
4. Chaum, D. (1985). Security without identification: transaction systems to make Big Brother obsolete. *Communications of the ACM*, 28(10), 1030–1044. <https://doi.org/10.1145/4372.4373>
5. Data (Use and Access) Act 2025, c. 18, section 81: Data protection by design: children's higher protection matters. Royal Assent 19 June 2025. legislation.gov.uk/ukpga/2025/18/section/81
6. Drachsler, H. and Greller, W. (2016). Privacy and analytics: it's a DELICATE issue. A checklist for trusted learning analytics. *Proceedings of LAK16*, 89–98. <https://doi.org/10.1145/2883851.2883893>
7. Hamari, J., Koivisto, J. and Sarsa, H. (2014). Does gamification work? A literature review of empirical studies on gamification. *47th Hawaii International Conference on System Sciences*, 3025–3034. <https://doi.org/10.1109/HICSS.2014.377>
8. Human Rights Watch (2022). "How Dare They Peep into My Private Life?" *Children's rights violations by governments that endorsed online learning during the Covid-19 pandemic*. 25 May 2022. docs.edtechhub.org/lib/SH2GMWNM
9. Information Commissioner's Office (2020). *Age appropriate design: a code of practice for online services*. Conformance expected from 2 September 2021. ico.org.uk
10. Information Commissioner's Office. *Principle (c): Data minimisation*. UK GDPR guidance. ico.org.uk
11. Kleppmann, M., Wiggins, A., van Hardenberg, P. and McGranaghan, M. (2019). Local-first software: you own your data, in spite of the cloud. *Proceedings of Onward! 2019*, 154–178. <https://doi.org/10.1145/3359591.3359737>
12. MongoDB. *Right to erasure with client-side field level encryption*. Documentation. mongodb.com/docs
13. Seald. *Data destruction using crypto-shredding*. seald.io/blog
14. Tennison, J. (ed.). *Good Practices for Capability URLs*. W3C Technical Architecture Group Finding (first draft 2014). w3.org/2001/taag/doc/capability-urls
15. UK General Data Protection Regulation, Article 5 (principles) and Article 25 (data protection by design and by default). legislation.gov.uk/eur/2016/679/article/5
16. W3C (2025). *Verifiable Credentials Data Model v2.0*. W3C Recommendation, 15 May 2025. Eds. Sporny, M., Thibodeau Jr, T., Herman, I., Cohen, G. and Jones, M. B. w3.org/TR/vc-data-model-2.0
17. Video game password saves: Tedium (2019), *Video game save state history*, tedium.co; Mental Floss, *Who was Metroid's Justin Bailey?*, mentalfloss.com

Patents (Table 1): US 11,100,754 B2 and US 2021/0383646 A1 (Aristocrat Technologies Australia; inventors Boesen and Chim); US 6,923,721 B2 (Sierra Design Group; inventors Luciano and Crowder); US 8,365,081 B1 (Amazon Technologies; inventors Amacker, Dicker and Snodgrass); US 8,949,610 B2 (National Chiao Tung University; inventors Lee and Tsai); US 8,984,650, US 9,542,573 and US 9,807,061 (Pearson Education); US 2012/0093318 A1 (SandForce, later LSI; inventor Obukhov); US 2013/0305057 A1 (IBM; inventors Greco and Jaquette). All available at patents.google.com.