Title: Smart Check Licensee Partner Policy

Date: 19th March 2026

Version: 1.4

Issued by: Construction Skills Certification Scheme Limited (CSCS)

---

1. Definitions

For the purposes of this policy:

"IT Partner"
means an organisation that designs, develops, integrates, operates, or supports software, systems, or services that connect to, or make use of, the CSCS Smart Check API or related Smart Check services, whether acting on behalf of a Service User or as part of its own integrated solution.

An IT Partner may include, without limitation, providers of access control systems, workforce management platforms, mobile applications, or other technical services that enable Smart Check card validation.

"Service User"
means the employer, principal contractor, or other organisation that uses the CSCS Smart Check service to validate cards in order to meet its legal, regulatory, or operational obligations in relation to site access, induction, or competence verification.

For clarity, the Service User is the end user organisation responsible for the card-reading activity and its lawful purpose, regardless of whether the Smart Check integration is delivered directly or via an IT Partner.

2. Purpose and status of this policy

This policy sets out **mandatory compliance and assurance requirements** for IT Partners who integrate with, or operate systems connected to, the CSCS Smart Check service.

The policy is intended to:

- Provide operational and governance expectations that **sit alongside**, but do not repeat, the Licence Agreement.
- Ensure consistent, lawful, and proportionate use of Smart Check services.
- Protect card holders, service users, and CSCS from misuse, data protection breaches, or security incidents.

Compliance with this policy is a **condition of continued access** to the Smart Check API and related services.

3. Lawful and permitted use of Smart Check

IT Partners must ensure that Smart Check is used **only for clearly defined, lawful purposes** that align with the service user's obligations as an employer or principal contractor.

In particular, they must ensure that the systems they design, integrate, or operate:

- Support **specific, legitimate card-reading events**, such as site access, induction, or qualification checks.
- Do **not** facilitate routine or speculative scanning of individuals who are not actively working on, or attending, a site.
- Do **not** enable continuous, excessive, or automated card reads without a clear operational justification.

4. Data protection and GDPR assurance

IT Partners must operate in a manner that enables service users and CSCS to meet their obligations under UK data protection law.

At a minimum, they must:

- Ensure Smart Check data is processed **only for the purpose of card validation and associated compliance activities**.
- Support the principle of **data minimisation**, ensuring that only the data required for a specific card read is processed or retained.
- Ensure that any additional data captured (such as read purpose or site context) is collected **solely to demonstrate lawful use and regulatory compliance**, not for profiling or secondary use.

IT Partners must maintain documented evidence of:

- Their role and responsibilities in relation to personal data.
- How lawful purpose is enforced within their systems.
- How data access is restricted to authorised users on a need-to-know basis.

5. Information security and organisational controls

IT Partners must maintain **appropriate and proportionate security controls** to protect Smart Check integrations and any associated data flows.

This includes, but is not limited to:

- Defined security ownership and accountability within the organisation.
- Secure system configuration and access controls.
- Monitoring and logging sufficient to identify misuse, abnormal activity, or attempted abuse of the service.
- Secure development and change management practices for any software interacting with Smart Check.

The objective is not to mandate a specific security standard, but to ensure IT Partners can **demonstrate reasonable, industry-aligned security practices** appropriate to the sensitivity of the service.

6. Incident and breach reporting

IT Partners must notify CSCS **immediately, in writing,** if they become aware of:

- Any actual or suspected security incident affecting Smart Check integrations.
- Any personal data breach, or suspected breach, involving Smart Check-related data.
- Any misuse of the Smart Check service that could impact card holders, service users, or CSCS.

Notifications must be made **without undue delay**, include known facts at the time, and be followed by timely updates as investigations progress.

IT Partners must cooperate fully with CSCS in:

- Incident investigation.
- Containment and remediation activities.
- Regulatory or stakeholder communications, where required.

7. Assurance, audit, and cooperation

IT Partners must be able to provide CSCS, on reasonable request, with evidence demonstrating:

- Compliance with this policy.
- Ongoing adherence to lawful use requirements.
- The existence and operation of appropriate security and data protection controls.

This may include high-level policies, attestations, or summaries of controls, rather than intrusive technical audits, unless risk or circumstances justify further assurance.

8. Notification of personnel changes and access removal

IT Partners must inform CSCS promptly when any individual within their organisation who has access to CSCS Smart Check resources leaves the organisation, changes role, or no longer requires access.

This includes access to, but is not limited to:

- Smart Check API documentation
- CSCS support systems
- CSCS Jira or issue-tracking systems
- Any other CSCS systems, tools, or documentation provided in support of Smart Check

Notification must be made by raising a support ticket via the CSCS support channel and must include:

- The name of the organisation
- The name of the individual whose access should be removed
- The date the individual left the organisation or ceased to require access

IT Partners are responsible for ensuring that access rights are kept accurate and up to date.

Failure to notify CSCS of personnel changes may result in unauthorised access remaining in place and may be treated as a security and compliance issue.

9. Access to API documentation and support

Access to CSCS Smart Check API documentation is restricted to authorised Service Users and IT Partners with a valid licence arrangement in place with CSCS.

API documentation is provided solely to support the permitted integration and operation of Smart Check and must be treated as confidential. It must not be shared with third parties or made publicly available.

Where access to API documentation is required, an existing authorised user within the Service User or IT Partner organisation must request access by raising a support ticket via the CSCS support channel. Requests should include the organisation name, the individual requiring access, and the reason access is needed. Access will be granted where appropriate and may be withdrawn if no longer required.

IT Partners and Service Users are responsible for ensuring that access to documentation is limited to individuals who genuinely require it and that documentation is stored securely.

The documentation is available at: API Documentation (only available to IT Partners with Confluence access)

10. Service availability, fault reporting and issue escalation

a. General approach

CSCS Smart Check is an aggregation service that relies on underlying data and services provided by individual card schemes.

IT Partners and Service Users should distinguish between:

- Issues affecting the Smart Check API service itself, and
- Issues relating to individual card scheme data or scheme systems.

This distinction is important to ensure issues are reported and resolved through the appropriate channel.

b. Reporting suspected Smart Check API faults

IT Partners should report issues to CSCS where there is a reasonable indication that the Smart Check API or its supporting services are not operating as intended.

Examples include, but are not limited to:

- The API is unavailable or consistently returning errors.
- Authentication or authorisation failures affecting multiple requests.
- Unexpected or inconsistent responses affecting multiple card reads or service users.
- Performance degradation or timeouts that prevent normal operation.

Faults should be reported promptly via the CSCS support channel, providing:

- A clear description of the issue observed.
- The date and time the issue occurred.
- Any relevant error codes or messages.
- Confirmation of whether the issue affects multiple cards, sites, or service users.

IT Partners should take reasonable steps to verify the issue before reporting, including confirming that the problem is not caused by local configuration, network issues, or misuse of the API.

The URL to report issues is: Report API Faults (only available to IT Partners with Jira access)

c. Single card or scheme-specific issues

Where a single card fails to validate via Smart Check, but the same card validates successfully when checked directly using the relevant scheme's own website or tools, this is unlikely to be a Smart Check API fault.

In such cases:

- The issue is likely to relate to the individual card scheme's data or systems.
- The IT Partner or Service User should contact the relevant card scheme directly for investigation and resolution.
- CSCS should not be treated as the first point of contact for scheme-specific card discrepancies.

This approach avoids unnecessary escalation and ensures issues are handled by the organisation best placed to resolve them.

d. Good practice expectations

IT Partners are expected to:

- Implement basic validation and error handling within their systems.
- Avoid raising support requests for isolated card issues without initial verification.
- Ensure operational teams understand the difference between Smart Check service issues and scheme-level card issues.
- Provide as much information as possible.

Failure to follow this approach may delay resolution and impact service availability for others.

11. Consequences of non-compliance

Failure to comply with this policy may result in:

- Required remedial actions within defined timescales.
- Suspension or restriction of Smart Check access.
- Escalation under the Licence Agreement where non-compliance presents material risk.

12. Review and updates

This policy may be updated by CSCS from time to time to reflect:

- Regulatory change.
- Evolving security threats.
- Lessons learned from incidents or consultation feedback.

IT Partners are responsible for ensuring continued compliance with the current version.