

Innovative Technology Ltd – Public Practice Statement

About this Public Practice Statement

This Public Practice Statement provides a certified, informative summary of the Practice Statement identified by Data Protection and Privacy, ICU Age Estimation 9 July 2026

The full Practice Statement and the underlying product, process or service has been assessed by the ACCS Certification Scheme and has met the applicable requirements of ACCS 1:2025 and ISO/IEC 27566-1:2025 - Age Assurance Systems - Part 1: Framework in accordance with scope of certification set out on their certificate and schedule.

The full Practice Statement contains sensitive, confidential or security-related information and is therefore not published. This public version provides information about the certified service while protecting information that should not be made publicly available.

For further information about the service, including enquiries about aspects of its operation that are not covered in this public summary, please contact the certified organisation directly.

Name of Client	Innovative Technology Ltd
Public Practice Statement Title	Data Protection and Privacy, ICU Age Estimation
Public Practice Statement Version	9 July 2026
Public Practice Statement Date	9 July 2026
Date Certified	6th August 2026

Data Protection and Privacy

ICU edge solution for age estimation

Company	Innovative Technology Limited
Company number	01954947
Registered office	Innovative Business Park, Derker Street, Oldham, Lancashire, OL1 4EQ
Product	ICU edge solution for local age estimation
ICO registration number	Z9777147
ICO date registered	23 May 2007
ICO registration expires	22 May 2027
Payment tier	Tier 2
Document status	Revised draft for ITL/DPO approval - ISO/IEC 27566-1:2025 aligned

Author	Andrew O'Brien
Original approval	Tom Pennington-Brookfield (DPO)

Confidentiality: this document is intended to support ITL product assurance and customer due diligence. It is not a substitute for controller-specific legal advice or deployment-specific DPIA/LIA approval.

Change log

Area	Change applied	Owner	Date
Cover page	Updated registered office wording and document status; retained ICO registration details from source document.	Andrew O'Brien	06/07/2026
Privacy position	Replaced absolute anonymity wording with a more precise privacy-by-design explanation covering transient processing and non-identification.	Andrew O'Brien	06/07/2026
ICO guidance	Updated references to the 2024 ICO age assurance opinion and ICO biometric data guidance.	Andrew O'Brien	06/07/2026
Lawful basis	Reconciled legitimate interests, legal obligation, consent, Article 9 and Article 22 considerations; added controller lawful-basis decision path.	Andrew O'Brien	06/07/2026
DPIA	Expanded DPIA risks, mitigations, residual risk, and controller deployment responsibilities.	Andrew O'Brien	06/07/2026
Accuracy and bias	Added methodology caveats and challenge-route controls; retained available ACCS and internal validation metrics.	Andrew O'Brien	06/07/2026
LIA template	Removed unfinished customer placeholders and replaced with controller deployment guidance.	Andrew O'Brien	06/07/2026
Complaints	Updated complaint handling section and ICO contact details.	Andrew O'Brien	06/07/2026
Layout	Applied formal ITL cover, header, footer, section structure, tables, captions, and accessible image alt text.	Andrew O'Brien	06/07/2026
ISO/IEC 27566-1 alignment	Added age assurance framework alignment, terminology, functional/performance/privacy/security/acceptability controls, practice statement guidance, fail-safe and audit-log considerations.	Andrew O'Brien	09/07/2026
Age check practice statement	Added an explicit binding description explaining how the age assurance result relates to the correct individual/current presentation, including result use, replay/reuse controls and relying party responsibilities.	Andrew O'Brien	09/07/2026
Collaborative attack prevention	Added explicit ACPS wording explaining how the standard local age estimation configuration reduces collaborative attacks through point-of-presentation binding, single-use results, active-face controls, staff supervision, challenge routes and controller integration controls.	Andrew O'Brien	09/07/2026

Contents

1. Purpose and scope
 2. Age check practice statement
 3. Definitions
 4. Relying party use cases
 5. Data protection classification and lawful basis
 6. Age check process overview
 7. User privacy by design
 8. Accuracy, bias and challenge handling
 9. Security, presentation attacks and cyber controls
 10. DPO, training, data sharing and penetration testing
 11. DPIA for ICU product range
 12. Controller deployment and LIA guidance
 13. Complaints and escalation
- Appendix A. Deployment transparency notice
- Appendix B. References
- Appendix C. ICU data lifecycle summary
- Appendix D. ISO/IEC 27566-1:2025 framework alignment checklist

1. Purpose and scope

This document describes the data protection and privacy controls for the ICU edge solution used for facial age estimation in age-restricted retail and venue environments. It is written for ITL internal governance, certification evidence, customer due diligence and deployment planning.

It also maps the standard ICU age estimation configuration to the ISO/IEC 27566-1:2025 age assurance framework at a product-assurance level. The alignment is presented as supporting evidence only; it does not claim formal ISO certification and does not replace the relying party's own practice statement or deployment assessment.

The standard ICU deployment performs age estimation locally on the device. It is not designed to identify, authenticate, recognise, track or enrol a person. It does not create or retain biometric templates, persistent identifiers, facial images, landmarks or transaction-level personal records after the check has completed.

This document supports, but does not replace, a controller-specific assessment. Each relying party remains responsible for assessing its actual deployment context, notices, lawful basis, challenge route, staff process and any integration with host systems or point-of-sale processes.

Key position: ITL treats transient facial age estimation as a data protection relevant process and designs the product to minimise privacy impact. The standard product configuration is not intended to carry out biometric recognition or special category biometric data processing because it is not used for unique identification.

2. Age check practice statement

The ICU devices (including MyCheckr, MyCheckr Mini and ICU Lite configurations where applicable) perform facial analysis on a subject to estimate age. The age estimation is carried out on local hardware. Data used for facial analysis is held transiently in working memory for the duration of the calculation and is automatically purged once the estimation result is produced.

Each presentation to the camera is treated as a new event. The device does not retain information that enables a later presentation to be linked back to an earlier presentation.

The product is intended to assist staff and premises in applying age-restriction policies such as Challenge 25. It is an aid to decision-making and should be deployed with an appropriate human challenge route, signage and alternative process where a customer objects or where the system cannot return a reliable result.

Certification context

This document is aligned with ACCS 2:2021 Technical Requirements for Data Protection and Privacy and supports the ICU age estimation certification evidence pack. Accuracy evidence is also described by reference to ACCS 1:2020 Technical Requirements for Age Estimation Technologies where available. The structure has also been reviewed against ISO/IEC 27566-1:2025, which frames age assurance systems around functional, performance, privacy, security, acceptability and practice-statement characteristics.

2.1 ISO/IEC 27566-1:2025 framework alignment

ISO/IEC 27566-1:2025 describes age assurance systems using functional, performance, privacy, security and acceptability characteristics, supported by practice statements. The table below summarises the product-level alignment for the standard ICU age estimation configuration.

ISO framework area	ICU product-level position
Functional	Local age estimation returns an age estimate or threshold result for the relying party workflow.
Performance	Accuracy evidence, challenge thresholds and demographic monitoring are documented.
Privacy	Local processing, minimisation, non-retention and non-identification are documented.
Security	PAD, input controls, access control, update governance and fail-safe expectations are documented.
Acceptability	Signage, alternative process, staff challenge route and complaint escalation are documented.
Practice statements	This document supports product-level evidence; relying parties complete deployment-specific documentation.

2.2 Binding of age assurance result to the correct individual

For the standard ICU age estimation configuration, binding is achieved at the point of presentation rather than by creating a persistent identity record. The person who presents to the device is the person whose active face is processed, and the age assurance result is returned only for that live/current presentation.

The device selects the active face in the camera frame using proximity, pose, size, sharpness and presentation-attack quality checks. This reduces the risk that the result relates to a bystander or another person in the background. If the device cannot establish a usable active presentation, it should not return a reliable pass result and the relying party should use staff review or an alternative age-check route.

The standard configuration does not bind the result using a biometric template, account identifier, reusable token or stored user profile. This is intentional: it supports non-identification and avoids adding to the individual's digital footprint. The result should therefore be treated as a single-use result for the current interaction only.

Relying parties and integrators must ensure the host workflow uses the result only for the person currently presenting to the device and only for the relevant transaction or access decision. A result must not be replayed, forwarded to another workflow, reused for a later presentation, linked to a customer account or used as evidence of identity unless that change has been separately assessed and documented through lawful-basis review, DPIA, security review and updated transparency information.

Binding element	Control / explanation
Subject binding	The active face currently presented to the camera is the subject of the age estimate.
Result binding	The result is linked to the current presentation and configured host workflow, not to a stored identity profile.
Single-use expectation	The result should be used promptly for the current transaction or access decision and should not be reused for another person or later event.
No persistent identifier	The standard configuration does not create a biometric template, user account, reusable token or persistent identifier for the person checked.
Fallback route	Where binding is uncertain, quality checks fail, spoofing is suspected or the result is disputed, staff should use ID challenge or another approved age-assurance method.
Controller responsibility	Any host logging, account linking, result reuse or automated final decision must be assessed and documented by the relying party/controller before deployment.

2.3 Collaborative attack prevention

Collaborative attacks are scenarios where more than one person attempts to misuse the age assurance process, for example where an adult presents to the device on behalf of an underage person, a valid result is shared or replayed for another person, or a host workflow attempts to treat a result as reusable evidence for a later transaction.

In the standard ICU local age estimation configuration, the system reduces collaborative attack risk by binding the result to the current live presentation and by not creating a reusable credential, account record, biometric template or persistent identifier. The active face must be presented to the camera and pass pose, size, sharpness and presentation-attack quality checks before a result is returned.

Because the standard configuration is intentionally non-identifying, it does not prove civil identity and it does not prevent every social or operational form of collusion on its own. Relying parties must therefore implement operational controls so that staff use the result only for the person physically presenting at the device and only for the current age-related eligibility decision.

Collaborative attack scenario	Prevention / control in standard deployment
Adult presents on behalf of an underage person	Result should be accepted only where the person presenting to the camera is the person seeking access. Staff supervision, device placement and transaction flow should prevent a second person substituting themselves for the customer.
Result shared with another person	The result is not a reusable age credential. It should be consumed immediately by the configured workflow and not displayed, stored, printed, forwarded or transferred for use by another person.
Replay of a previous result	Each presentation is treated as a new event. A previous pass result must not be treated as valid for a later presentation unless the relying party has separately assessed, documented and controlled that reuse.
Bystander or group presentation	Active-face selection and quality checks reduce the risk of processing a person in the background. Where multiple faces, poor pose or uncertain presentation conditions affect confidence, staff should use manual challenge or an alternative route.
Staff or host workflow misuse	Integrators should restrict result handling to the configured age-check workflow, apply role-based access where systems are used, and prohibit account linking, manual override misuse or onward use without reassessment.
Indeterminate, suspicious or inconsistent context	Quality failure, suspected spoofing, unusual presentation behaviour or mismatch with the transaction context should trigger fail-safe handling, staff review, ID check or another age assurance method.

These controls are intended to reduce collaborative attack risk while preserving the privacy-by-design position of the standard configuration. If a relying party requires stronger assurance that the same person remains bound across multiple transactions, that would be a material change and should be assessed separately because it may introduce identification, persistent identifiers or additional personal data processing.

3. Definitions

Term	Definition
Device	The local hardware component of the ICU solution, including ICU Pro or ICU Lite variants where applicable.
Facial analysis	Processing facial features or facial-derived measurements to perform a function such as age estimation. In this deployment, facial analysis is not used for identity recognition.
Age estimation	An automated estimate of apparent age based on facial cues. It is not proof of identity or date of birth.
Biometric recognition	Automated recognition of a person based on biological or behavioural characteristics for the purpose of identifying, authenticating or recognising that person. The standard ICU age estimation configuration is not designed for this purpose.
Transient data	Data held temporarily in working memory solely to complete the age estimate, then automatically deleted.
GDPR / UK GDPR	The UK General Data Protection Regulation and related UK data protection legislation, including the Data Protection Act 2018.
UVC v1.5	USB Video Class standard protocol used by USB cameras to transfer camera data to a connected device.
PAD	Presentation Attack Detection controls intended to detect non-live or spoofed presentation attempts such as printed photographs or screen replays.
Age assurance	Processes and methods used to verify, estimate or infer age or age range for an age-related eligibility decision.
Age assurance result	The output used by a relying party, such as an age estimate, over-threshold result or under-threshold result.
Relying party	The organisation using the result to decide access to age-restricted goods, services, venues or spaces.
Age-related eligibility decision	A decision about access based on whether the person meets an age threshold or age range requirement.

Term	Definition
Binding	Controls that ensure the age assurance result relates to the person presenting to the system.
Indicator of effectiveness	A measure used to assess whether an age assurance characteristic is achieved, such as classification accuracy, error rates or fairness monitoring.
Digital footprint	Information created or retained about an individual through interaction with a device or service.
Fail safe	System behaviour where failure does not produce an unsafe age assurance result or expose additional personal data.
Practice statement	A document describing the practices, procedures and controls used by a provider or relying party for age assurance.

4. Relying party use cases

For relying parties and their users, privacy, proportionality and non-identification are important deployment factors. The product is designed to estimate age without requiring users to disclose official identification documents for every transaction and without retaining data from the check.

Application	Indicative legislation / context	Access age	Typical challenge age
Alcohol	Licensing Act 2003	18	25
Gambling / betting / lottery	Gambling Act 2005 and applicable licence conditions	18	25
Tobacco and e-cigarettes	Children and Young Persons (Protection from Tobacco) Act 1991 and related legislation	18	25
Intoxicating substances	Intoxicating Substances (Supply) Act 1985	18	25
Knives and offensive weapons	Criminal Justice Act 1988, Knives Act 1997, Offensive Weapons Act 1996 and related restrictions	18	25
Fireworks	Fireworks (Safety) Regulations 1997 and related requirements	18	25

5. Data protection classification and lawful basis

5.1 Personal data, biometric data and special category data

The system processes a live camera image and facial-derived features for less than the duration required to return an age estimate. During that brief processing window, ITL takes a cautious approach and treats the data protection principles as relevant because a person may be identifiable in context even though the product does not retain data after the check.

The standard ICU age estimation deployment does not create or compare biometric templates and is not intended to identify, authenticate, recognise, enrol or track an individual. On that basis, it is not intended to process special category biometric data for the purpose of uniquely identifying a natural person.

If a customer, integrator or relying party changes the deployment so that images, templates, age results, transaction logs or other identifiers are linked to an identifiable person, the controller must reassess the processing before deployment. That reassessment should include lawful basis, any Article 9 condition, DPIA, retention, transparency, data subject rights, security controls and contractual responsibilities.

Question	Standard ICU position	Controller action if deployment changes
Does the product identify a person?	No. It returns an age estimate and does not match the user to a stored identity.	Reassess as biometric recognition if identification, authentication or tracking is introduced.
Are images stored?	No. Images are processed locally and deleted after the estimate.	Define retention, access controls, transparency and lawful basis before any storage is enabled.
Are biometric templates created?	No persistent biometric template is created or retained.	Treat template creation as high-risk and reassess Article 9 and DPIA obligations.
Can results be linked to a customer account?	Not in the standard product configuration.	Controller must assess additional personal data processing and update notices/contracts.

5.2 Lawful basis

The lawful basis depends on the relying party deployment. For many age-restricted retail deployments, the controller is likely to consider Article 6(1)(f) legitimate interests or, where a specific legal obligation applies to the age assurance processing, Article 6(1)(c) legal obligation. The controller must document the basis that best reflects the actual purpose and relationship with customers.

Where legitimate interests is used, the controller should document the three-part test: purpose, necessity and balancing. The purpose is to restrict access to age-restricted goods or services and support staff compliance. The necessity test should explain why local age estimation is a proportionate first-stage check compared with checking identity documents for every customer. The balancing test should account for children, vulnerable customers, privacy expectations, transparency, short processing duration, non-retention, bias testing and challenge routes.

Consent should not be treated as a default solution where the age check is effectively mandatory for a transaction. If a controller chooses a consent-based route for a specific deployment, it must ensure consent is freely given, specific, informed and withdrawable, with a genuine alternative process available.

Basis / condition	When it may be relevant	Deployment note
Article 6(1)(f) legitimate interests	Common candidate for first-stage age estimation in age-restricted retail contexts.	Requires documented LIA and balancing against user rights and freedoms.
Article 6(1)(c) legal obligation	May be relevant where the controller is legally required to carry out age checks in a specific context.	Controller must identify the specific legal obligation and necessity.
Article 9 condition	Required where the deployment processes special category data, including biometric data used for unique identification.	Standard ICU age estimation is not intended for unique identification; any deviation, such as facial recognition, enrolment, template creation, account linking or retained images, requires reassessment.
Consent / explicit consent	May be used in some voluntary or optional deployments.	Not recommended as a blanket basis for mandatory retail age checks unless a genuine alternative is available.

5.3 Controller lawful-basis decision path

The controller must identify and document the lawful basis before deploying the ICU age estimation system. The appropriate lawful basis depends on the actual deployment, the age-restricted product or service, the legal duties applying to the relying party, and whether the result is used only as a first-stage age check or as part of a wider customer-identifiable workflow.

For standard local age estimation, where the device processes a live facial image transiently and returns only an age estimate or age-threshold result, the likely Article 6 basis will usually be either legitimate interests or legal obligation.

Where legitimate interests is selected, the controller should complete a Legitimate Interests Assessment covering the purpose of preventing underage access to age-restricted goods or services; why local age estimation is necessary and proportionate compared with routine ID checks for every customer; and why the interests, rights and freedoms of customers do not override the controller's interest, taking account of safeguards such as local processing, no retained images, no biometric templates, signage, human challenge routes, bias monitoring and alternative age-check processes.

Where legal obligation is selected, the controller must identify the specific legal or regulatory obligation that requires age assurance and explain why the ICU processing is necessary to meet that obligation. The controller should also assess when that obligation has been discharged and whether any further processing by a host system requires a separate lawful basis.

Consent should not be used as the default lawful basis for mandatory age checks. If consent is used for a specific optional deployment, the controller must ensure that consent is freely given, specific, informed, unambiguous, withdrawable and supported by a genuine alternative route.

Article 9 is not expected to apply to the standard ICU age estimation configuration because the device is not intended to uniquely identify a person. Article 9 must be reassessed if the deployment introduces facial recognition, enrolment, biometric templates, customer account linking, persistent identifiers, retained images or any other processing that enables unique identification.

The controller must also consider whether the deployment involves solely automated decision-making with legal or similarly significant effects. Where the ICU output is used only to trigger staff review or a manual age/ID check, this risk is reduced. If the system is configured to make final automated access decisions without meaningful human review, the controller must complete an Article 22 assessment and document the safeguards in place.

6. Age check process overview

The ICU solution operates offline and performs age estimation on local hardware. A USB camera passes images to the ICU device over a closed UVC connection. The host system receives only the returned age estimate or age-threshold result required for the configured workflow.

Processing is limited to one active face per frame. The active face is the face closest to the camera that passes quality checks such as pose angle, face size, sharpness and presentation attack detection. This approach reduces the risk of processing bystanders or people passing in the background.

Step	Processing action	Privacy control
1	Camera stream is received by ICU hardware via UVC.	Closed direct connection; no remote processing required.
2	Face detection identifies whether a usable face is present.	Only the active face meeting quality checks is processed.
3	Landmarks and quality checks are calculated.	Landmark data is transient and used only to support the age estimate.
4	If quality criteria are met, the estimation algorithm returns an age estimate or threshold result.	Only the result required by the relying party workflow is returned.
5	Transient image and landmark data is deleted from working memory.	No persistent images, templates or personal identifiers are retained by the device.

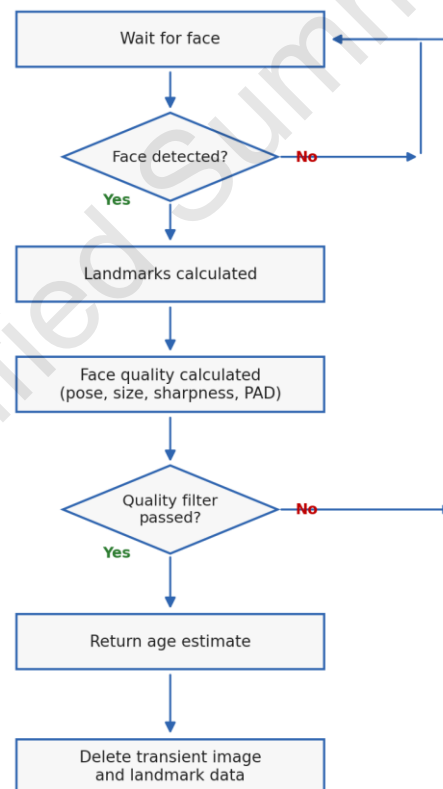


Figure 1: Process pipeline for local age estimation.

Frequency of re-check

No user profile or persistent record is stored on the ICU device. If the same person presents to the camera again, the system treats that as a new presentation and repeats the process from the beginning.

Binding and result delivery

For the standard local configuration, binding is achieved at the point of presentation: the device processes the active face presented to the camera and returns the current result to the configured workflow. The result should

be used promptly and should not be reused for another person or later transaction unless the relying party has separately assessed and documented a lawful reuse process. The practice-statement binding position is set out in Section 2.2 and is summarised below for the process flow.

ISO-related consideration	ICU / controller control
Correct binding	Use the result only for the person currently presenting to the device.
Secure result delivery	Return only the configured age estimate or threshold result to the host workflow.
Replay or reuse	Do not treat a previous result as valid for a new person or transaction unless assessed.
Indeterminate result	Use manual challenge or an alternative age assurance route where the device cannot return a reliable result.

7. User privacy by design

Principle	Implementation in standard ICU deployment
Purpose limitation	Data is processed solely to estimate age or return an age-threshold result for age-restricted goods or services.
Data minimisation	The product avoids routine collection of identity documents and does not request name, date of birth, address or document numbers.
Storage limitation	Transient image and facial-derived data are deleted once the result has been produced.
Security by design	The system is designed for local/offline operation, controlled input sources and restricted administrative access.
Transparency	Relying parties should use signage and customer-facing notices explaining the age estimation process and alternative/challenge route.
Non-identification	No biometric templates, persistent identifiers or tracking mechanisms are created in the standard configuration.

ISO/IEC 27566-1:2025 privacy characteristics emphasise minimised collection, non-disclosure of unnecessary age-related data, purpose limitation, access control, disposal and avoidance of adding to an individual's digital footprint. The standard ICU configuration is aligned to those principles as summarised below.

Privacy characteristic	Standard ICU alignment / relying party note
Collection limitation	Only transient facial data needed to estimate age is processed by the device.
Non-disclosure	The relying party should receive only the result needed for the workflow, preferably a threshold result where a specific age is not necessary.
Purpose limitation	Data must not be repurposed for marketing, surveillance or identity recognition without reassessment.
Access control	Administrative access to device configuration, IMS and host integrations should be restricted.
Data disposal	Images, landmarks and facial-derived working data are deleted after the result.
Digital footprint	The standard device does not create persistent identifiers, user accounts or reusable tokens for the person being checked.
Audit logs	Where logs are required, they should avoid biometric images, identity document data and unnecessary personal identifiers.

Customers are provided with an information sticker to place near the system. The notice should be supplemented by the relying party's privacy information where local law, store layout or the deployment process requires more detail.



Figure 2: Customer-facing age estimation information sticker.

8. Accuracy, bias and challenge handling

The ICU age estimation system has been independently assessed and certified for deployment within a Challenge 25 retail environment by the Age Check Certification Scheme. Testing was conducted in accordance with ACCS 1:2020 Technical Requirements for Age Estimation Technologies.

The primary certification concern is whether a person at or near the legal threshold could be incorrectly classified as being above the Challenge 25 threshold. The system is intended to support staff, not remove the need for a clear human challenge route where a customer disputes the result or where the result is inconclusive.

In ISO/IEC 27566-1:2025 terms, performance should be expressed through indicators of effectiveness such as classification accuracy, false positive and false negative behaviour, fairness/error parity across demographic groups, response time and completion rate where relevant. For this product document, available ACCS and internal validation measures are used as product-level evidence; relying parties should monitor operational outcomes and complaints in deployment.

Performance characteristic		Evidence / control in this document
Classification accuracy		ACCS certification evidence and internal validation data are referenced; deployment changes should trigger review.
False positive / false negative impact		Challenge 25 threshold and staff escalation reduce unsafe access decisions and unfair denial.
Outcome error parity		Gender and skin-tone validation and complaint monitoring are used to identify differential performance.
Response time / completion		Device performance should remain suitable for retail/venue workflow and be reviewed after configuration or hardware changes.
Testability		Validation records, configuration records and deployment checks should be retained for audit and review.

Metric	Result	Interpretation / caveat
Actual age in ACCS sample	17.81 years	Nominally close to the legal access threshold.
Estimated age	18.20 years	Estimated age remained below the Challenge 25 policy threshold.
Delta	+0.39 years	Reported estimate was close to actual age for the tested sample.
Mean absolute error	0.94 years	Low MAE supports suitability, subject to methodology, population and ongoing monitoring.

Further internal testing has been carried out across ages 16 to 23 and demographic groupings. The figures below reproduce available internal validation data and should be read with the underlying test report, including sample size, collection methodology, demographic distribution, environmental conditions and confidence intervals where available.

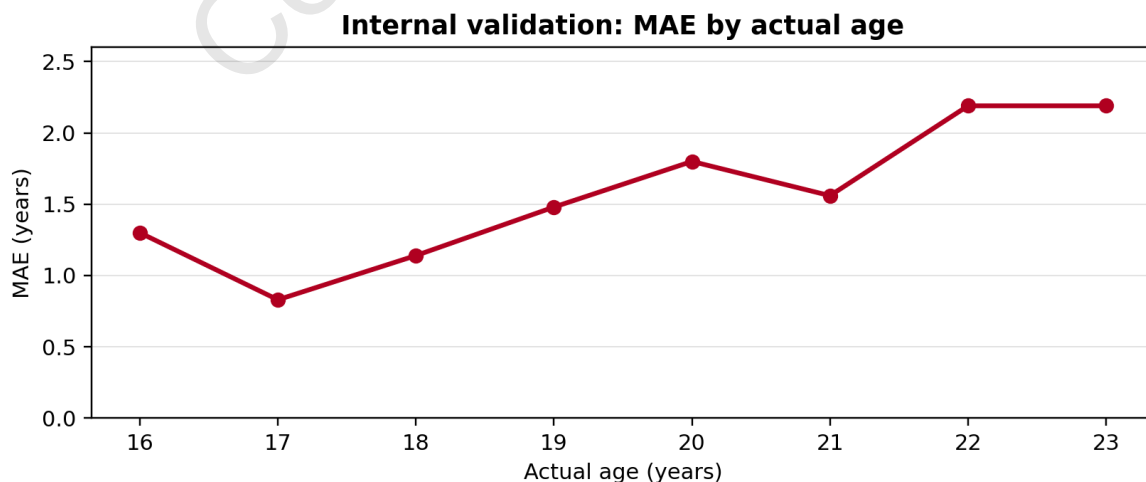


Figure 3: Internal validation MAE by actual age.

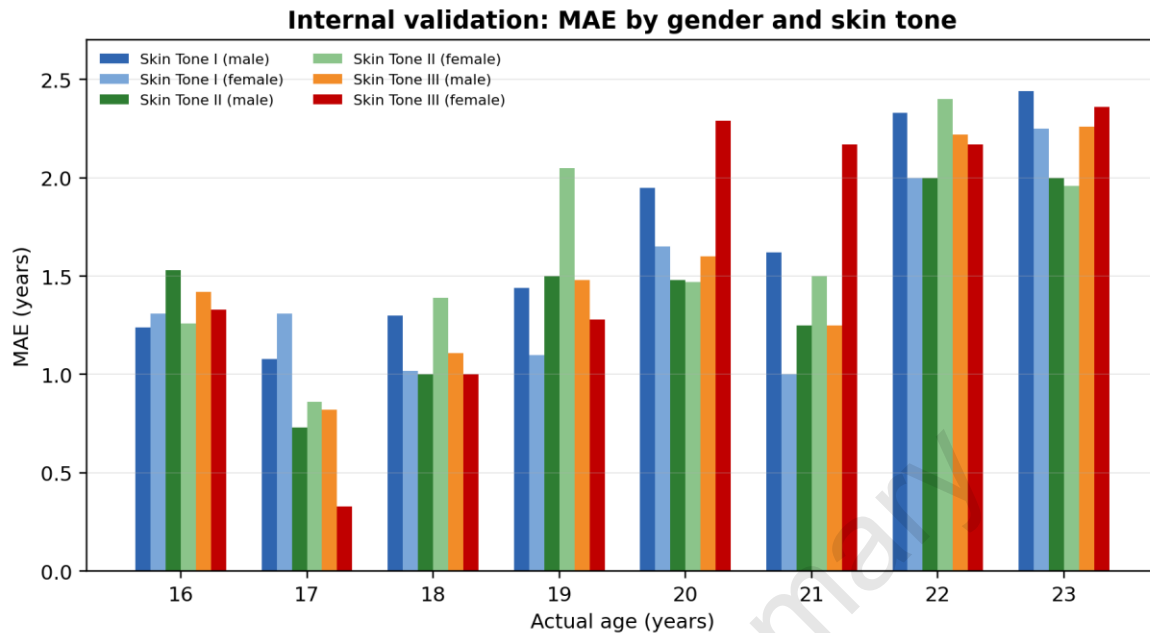


Figure 4: Internal validation MAE by gender and skin tone.

Control area	Control / requirement
Ongoing validation	Maintain test records across relevant age ranges, genders, skin tones and deployment environments.
Bias monitoring	Review differential performance and investigate any material performance gap.
Threshold configuration	Use Challenge 25 or equivalent policy thresholds to provide a safety margin above the legal access age.
Human challenge route	Staff must be able to request ID or use an alternative process where the result is disputed, inconclusive or inappropriate.
Complaint trigger	Complaints alleging bias, inaccuracy or ineffective challenge must trigger DPIA and remediation review.

9. Security, presentation attacks and cyber controls

The primary direct attack risk is a presentation attack, where a person attempts to deceive the age estimation system using a printed photograph, image on a mobile device, video replay or other non-live facial artefact.

ICU products include Passive Presentation Attack Detection (PAD) controls designed to identify and reject spoofing attempts. PAD is supported by neural network models trained to distinguish genuine presentations from artefacts, and by depth, texture and presentation cues where supported by the hardware and software configuration.

The system design also considers injection and cyber-attack vectors. These include attempts to introduce synthetic or manipulated data into the processing pipeline, bypass the camera input, gain unauthorised administrative access, or alter the device configuration.

Risk / attack vector	Mitigation
Printed photograph or screen replay	Passive PAD controls and quality checks reject non-live or low-quality presentations.
Background or bystander processing	Active face selection and pose/quality checks limit processing to the face intentionally presented to the device.
Data injection into processing pipeline	Input source controls, protected keys/passphrases and controlled host interface reduce bypass risk.
Remote cyber attack	Standard deployment is offline with no direct external network access to the ICU device.
Unauthorised physical access	Access requires physical connection and is password protected. Administrative access should be restricted to authorised personnel.
Host or IMS misuse	Where IMS is used for device access, credentials should be role-based, securely managed and removed when no longer required.
Configuration drift	Software/configuration updates should be controlled, recorded and reviewed for data protection impact.

ISO/IEC 27566-1:2025 also highlights replay, forwarding, reuse, contra indicators and fail-safe behaviour. These points are addressed at product and deployment level as follows.

Security characteristic	ICU / controller control
Replay / reuse	A current result should be tied to the current presentation and not reused for another person or transaction unless assessed.
Forwarding	Host integrations should prevent a result produced for one relying party workflow being forwarded for a different purpose.
Contra indicators	Quality failure, suspected spoofing or inconsistent context should trigger manual review or an alternative route.
Fail safe	If capture, processing, communication or configuration fails, the device should not produce an unsafe pass result.
Change control	Configuration changes affecting privacy, performance, security or acceptability should be recorded and reviewed.

10. DPO, training, data sharing and penetration testing

10.1 Appointment of DPO

ITL has appointed Tom Pennington-Brookfield as Data Protection Officer. The DPO reports to the ITL board and coordinates general GDPR training and data protection governance. The appointment also supports ACCS 2:2021 requirements where large-scale special category processing questions may arise in a customer deployment context.

The standard ICU deployment is designed not to process special category biometric data for unique identification. However, DPO oversight remains appropriate because age estimation using facial analysis can raise privacy, fairness and public trust concerns.

10.2 Training and education

There is no product-specific training on stored personal data within the ICU age estimation solution because the standard device does not store personal data after the check. Training instead focuses on privacy-by-design operation, signage, alternative challenge routes, handling customer objections, complaint escalation and general GDPR awareness.

Relying parties should train staff to understand that the device supports, but does not replace, a lawful and fair age-restriction process. Staff should know when to request ID, when to use an alternative route and how to escalate complaints.

10.3 Data sharing and international transfers

No facial images, biometric templates or facial-derived data are shared from the standard ICU age estimation solution because no such data is retained after processing. The standard product does not require international transfer of user facial data. Any customer integration that records, transmits or links age results to an identifiable person must be assessed separately by the controller before deployment.

10.4 Penetration testing and access controls

The ICU is designed as a closed, local system with a simple USB camera connection and physical access controls. Access to the unit is password protected. Security testing and change control should verify that host integration, IMS access, firmware/software updates and physical access remain consistent with the documented privacy posture.

11. DPIA for ICU product range

This DPIA section provides a product-level assessment for the ICU product range. It should be reviewed and adapted by each controller for its actual deployment, including premises layout, customer communications, staff process, host integration and jurisdiction-specific age-restriction requirements.

11.1 Need for a DPIA

The product analyses a person's face to estimate age. Although the standard product does not identify, authenticate or track an individual, facial analysis used for age assurance is privacy-sensitive and may affect children or vulnerable individuals. A DPIA is therefore recommended as a matter of accountability and privacy-by-design governance, and may be mandatory depending on the relying party deployment.

A DPIA must be completed where processing is likely to result in a high risk to individuals. Any integration that stores images, creates templates, links age results to customer records or uses the product for biometric recognition must be treated as a material change requiring a new DPIA and legal review.

11.2 Description of processing

Item	Description
Controller	Innovative Technology for ITL-controlled activities; relying party/customer for its in-store or venue deployment.
Data subjects	Visitors/customers presenting to the age estimation device. Children may be included where they attempt to access age-restricted goods or services.
Data processed	Live facial image and facial-derived measurements held transiently in local working memory; returned age estimate or threshold result.
Purpose	Assist in restricting access to age-restricted goods and services and support staff compliance with Challenge 25 or equivalent policies.
Processing location	Local device hardware; standard operation does not require internet access or remote processing.
Retention	No retained facial images, landmarks, templates or identifiers in the standard configuration.
Sharing	No facial data sharing in the standard configuration.

11.3 Necessity and proportionality

The objective is to support staff in preventing underage access to restricted goods and services while reducing unnecessary disclosure of full identity documents by customers who clearly exceed a challenge threshold. Compared with routine ID checks for all customers, local age estimation may reduce collection of names, dates of birth, document numbers, addresses and images of identity documents.

The proportionality of any deployment depends on clear signage, minimal data handling, local processing, no retention, appropriate thresholds, staff training, a human challenge route and a fair alternative for customers who object or cannot be assessed accurately.

11.4 Risks and mitigations

Risk	Potential impact	Likelihood before controls	Severity	Controls / mitigation	Residual risk
False acceptance	Underage person may not be challenged where the estimate is too high.	Medium	High	Challenge 25 threshold, ACCS testing, staff escalation, periodic accuracy review.	Low / Medium
False rejection / inconvenience	Adult customer may be challenged unnecessarily or delayed.	Medium	Low	Clear challenge process, alternative ID route, staff training.	Low
Bias or unfair performance	Different demographic groups may experience more errors or challenges.	Medium	Medium	Gender/skin tone validation, monitoring of complaints and trends, retraining and remediation.	Low / Medium
Excessive data collection	Customer may be asked for more personal data than required.	Low	Medium	Local age estimation, no ID document capture by device, data minimisation guidance.	Low
Poor transparency	Customer may not understand the age estimation process.	Medium	Medium	Sticker/signage, privacy information, staff explanation and complaint route.	Low
Unlawful function creep	Device could be integrated with systems that identify or track users.	Medium	High	Deployment controls, contractual limits, change control and DPIA trigger for integrations.	Low / Medium
Spoofing / presentation attack	System may be deceived by non-live facial artefact.	Medium	High	PAD, quality checks, controlled camera input and staff supervision.	Low / Medium
Unauthorised access / cyber compromise	Configuration or software could be altered or data pathway misused.	Low / Medium	High	Offline design, restricted physical access, password protection, host/IMS access controls, update governance.	Low / Medium
Ineffective complaint/challenge route	Users may be unable to contest an outcome or report harm.	Medium	Medium	Published complaint route, staff escalation, central complaint log and DPIA review trigger.	Low

12. Controller deployment and LIA guidance

The previous customer LIA template has been removed from the main document because controller-specific placeholders cannot be completed by ITL without knowing the relying party, premises, jurisdiction, sales process and alternatives offered. A controller should complete its own LIA or lawful-basis assessment before deployment.

ITL can provide product-level information to support that assessment, including local processing, no retained images or templates, age-restriction purpose, accuracy evidence, PAD controls, privacy notices and challenge process guidance.

LIA stage	Controller questions	Product-level information available from ITL
Purpose test	What legitimate interest is pursued and why is the age estimation needed?	Product supports prevention of underage access and reduces routine ID document disclosure.
Necessity test	Is the processing necessary and proportionate compared with alternatives?	Standard device performs local, transient age estimation and does not store images/templates.
Balancing test	Do user rights override the controller interest?	Safeguards include no retention, signage, challenge route, bias monitoring and alternative process.
Special category check	Does the actual deployment involve biometric recognition or unique identification?	Standard ICU configuration is not designed for unique identification; any change requires reassessment.
Transparency and rights	How will customers be informed and how can they challenge or object?	ITL provides sticker/notice content and recommended complaint triggers.

13. Complaints and escalation

All complaints relating to facial age estimation, age assurance or biometric processing must be assessed against the relevant DPIA, lawful-basis assessment, accuracy evidence, fairness testing, retention controls, transparency materials and challenge process.

Consistent with ISO/IEC 27566-1:2025 acceptability expectations, relying parties should provide an accessible complaint route, acknowledge complaints promptly, define whether the relying party or age assurance provider is responsible for each handling stage, and use complaint outcomes to improve the deployment and supporting practice statement.

Where the processing is not intended for unique identification, that position must be documented and kept under review. Any complaint suggesting inaccuracy, bias, excessive retention, poor transparency or ineffective challenge must trigger a DPIA review and remediation assessment. Outcomes from biometric or age assurance complaints must be logged centrally and reviewed for systemic trends.

Data subjects have the right to complain to the ICO if they are unhappy with how their data has been handled. Relying parties should also provide a direct local complaint route so issues can be resolved promptly.

ICO contact route	Details
Telephone	0303 123 1113
Textphone / Relay UK	Dial 18001 followed by 0330 123 1113
Hours	Monday to Friday, 9am to 5pm
Postal address	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Website	https://ico.org.uk/

Appendix A. Deployment transparency notice

The following model wording may be adapted by relying parties for customer-facing notices. It should be checked against the controller's privacy notice and deployment-specific assessment before use.

Notice area	Model wording
Short sign	Age estimation technology is in use. The system estimates age locally. No facial images or biometric templates are stored by the device after the check. Ask a member of staff for an alternative age-check route.
Privacy notice supplement	We use local age estimation to help apply age-restriction rules. The device analyses a live camera image only for long enough to return an age estimate or age-threshold result. The device is not used to identify you and does not keep your image after the check.
Challenge route	If you disagree with the result or do not want to use the age estimation device, please speak to a member of staff. You may be asked to provide accepted ID or use an alternative process.
Complaint route	If you have a data protection concern, contact the venue/controller using the details in its privacy notice. You can also complain to the ICO if you remain unhappy.

Appendix B. References

ACCS 2:2021 Technical Requirements for Data Protection and Privacy: Certification criteria approved by the Information Commissioner for UK GDPR Article 42 certification schemes.

ACCS 1:2020 Technical Requirements for Age Estimation Technologies: Performance criteria for age estimation technologies used in age-restricted scenarios.

ISO/IEC 27566-1:2025, Information security, cybersecurity and privacy protection - Age assurance systems - Part 1: Framework.

ICO, Age assurance for the Children's code: <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/>

ICO, Expectations for age assurance and data protection compliance: <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/6-expectations-for-age-assurance-and-data-protection-compliance/>

ICO, Biometric data guidance: biometric recognition: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>

ICO, Key data protection concepts for biometric data: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/key-data-protection-concepts/>

ICO, Data protection impact assessments: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/>

Companies House, Innovative Technology Limited company profile: <https://find-and-update.company-information.service.gov.uk/company/01954947>

ICO contact details: <https://ico.org.uk/global/contact-us/>

Appendix C. ICU data lifecycle summary

Data item	Created?	Stored?	Shared?	Retention
Live camera image	Yes, transiently during processing	No	No	Deleted from working memory after result
Face landmarks / quality metrics	Yes, transiently during processing	No	No	Deleted after result
Biometric template for recognition	No in standard configuration	No	No	Not applicable
Age estimate / threshold result	Yes	Not retained by the ICU device in standard configuration	Returned to configured host workflow	Controller must assess any host logging separately
Customer identity details	No	No	No	Not applicable

Appendix D. ISO/IEC 27566-1:2025 framework alignment checklist

This checklist is a product-level mapping to ISO/IEC 27566-1:2025. It is intended to help ITL, auditors and relying parties understand how the standard ICU age estimation configuration supports the age assurance framework. It does not replace a deployment-specific relying party practice statement.

Framework area	Document evidence / action
Age assurance method	ICU uses an age estimation method based on facial age analysis; it is not an identity-document age verification method.
Functional characteristics	Sections 2, 6 and 12 describe age assurance result, context of use, configuration/deployment responsibilities and controller assessment.
Binding	Sections 2.2 and 6 describe active-face processing, current-presentation use, single-use result handling and controller controls to prevent the result being reused for a different person or transaction.
Performance characteristics	Section 8 describes ACCS testing, internal validation, challenge margin, demographic monitoring and complaint triggers.
Privacy characteristics	Sections 5, 7 and Appendix C describe local processing, minimisation, non-retention, non-identification and lifecycle controls.
Security characteristics	Sections 2.3 and 9 describe PAD, spoofing controls, collaborative attack prevention, input controls, administrative access, update governance, contra indicators and fail-safe expectations.
Acceptability characteristics	Sections 7, 8, 10, 11, 13 and Appendix A describe transparency, user awareness, challenge route, alternative process, staff training and complaints.
Practice statement	Section 2 acts as provider product-level practice statement information, including method, context, binding approach and controls; relying parties must document deployment context, thresholds, lawful basis, configuration, binding use and redress process.
Audit and review	Sections 8, 9, 11 and 13 require validation records, configuration review, DPIA review triggers and complaint trend review.
Collaborative attack prevention	Section 2.3 describes controls against an adult or other person presenting on behalf of someone else, result sharing, replay, forwarding, account linking and misuse by host workflows or staff.

End of document