Regulatory Sandbox Final Report: Department for Education

A summary of the Department for Education's participation in the ICO's Regulatory Sandbox

Date: May 2025

Information Commissioner's Office

Contents

1. Introduction

1.1 The Regulatory Sandbox ('the Sandbox') is a service that the ICO provides to support organisations that are developing products or services which intend to use personal information in innovative and safe ways and will deliver a potential public benefit.

1.2 The Sandbox is a free, professional service that is available to organisations of all sizes who meet our entry criteria and specified areas of focus. These criteria are assessed by the Sandbox's application processes. You can read our entry criteria in our Guide to the Sandbox and our terms and conditions.

1.3 The Sandbox specifically seeks to engage with projects operating within challenging areas of data protection. Sandbox participants have the opportunity to engage with the ICO, draw upon its expertise and receive support on mitigating risks and implementing data protection by design and default into their product or service. This helps ensure that the participant identifies and implements appropriate protections and safeguards.

1.4 The Department for Education ('DfE') is a ministerial department responsible for children's services and education, including higher and further education policy in England. DfE entered the Sandbox to develop their 'Education Credential' which uses innovative concepts of decentralised identity and verified credentials to allow post-16 students ('learners') within the English education system to access, manage and share their information when applying and enrolling into further education institutions ('FEIs'). The aim of the education credential is to streamline existing application and enrolment processes that currently use time consuming methods such as paper-based forms, manual input and photocopying which duplicates effort. DfE's research showed that time spent by FEI administrative staff inputting data on results day reduces the available time to answer learners' questions about their course or to offer support finding suitable further education programmes for learners who are working out their options upon receipt of their exam results.

1.5 The ICO accepted DfE into the Sandbox in November 2023, determining that their development of the education credential aligned with the ICO's decentralised identity area of focus in place at the time of the application to the Sandbox.

1.6 The ICO and DfE agreed to work together on the following objectives:

- **Objective one**: Consider how the education credential will comply with key data protection principles such as lawfulness of processing.
- **Objective two:** Determine the roles and responsibilities of parties that use the education credential, looking at how each organisation can ensure that data subject rights are deliverable. Placing a specific focus on individual rights that are more challenging with this particular technology such as rectification, erasure and data portability.
- **Objective three:** Identify and address challenges related to providing effective information about the collection and processing of personal information in processing activities related to the education credential.
- **Objective four:** Explore key data protection risks posed by the use of verified credential technology and implement a 'data protection by design and default' approach to mitigate these risks.

1.7 The Sandbox work commenced in January 2024 and concluded in January 2025. This exit report summarises the work and key learnings during DfE's time in the Sandbox. It should be noted that the report is limited to the data protection objectives described above (1.6) and does not represent all the obligations an organisation may have to comply with data protection legislation.

1.8 With consultation from participating organisations, the Sandbox publishes exit reports for all participants so that fellow innovators facing similar questions about data protection by design can benefit from the key learnings from the Sandbox. It should be noted that the views in this report are based on the ICO's specific contextual understanding of DfE's operations and, therefore, it cannot be guaranteed that other organisations will be able to apply these considerations in the same way. Considerations in this report are subject to change as the data protection landscape in the UK evolves and as DfE updates their organisational practices.

2. Product description

2.1 Decentralised ID is a form of identity where identity-related information is unique, self-controlled, private and portable. The implementation varies from protocol to protocol, but the underlying idea remains the same. The identifier in DfE's education credential is a person's Unique Pupil Number (UPN) / Unique Learner Number (ULN).

2.2 Verifiable Credential, referred to as an 'Education Credential' by DfE, is a set of credentials that can be securely and strongly verified by a relying party (RP). In this case the RP is the FEI. There can be varying levels of flexibility in terms of issuing/reissuing, rectifying and deletion of each of the credentials stored in the wallet. For example, examination scores and contact details will have different verification requirements and levels of proof required in order for an updated credential to be reissued. Verified credentials use open protocols to promote interoperability as the more organisations that are able to receive the credential will give more people control to share their information with the organisations they choose. Here, the use of a verified credential facilitates learners sharing their data between FEIs.

2.3 DfE has opted to use a permissioned blockchain structure with managed access for specific actors such as schools and FEIs to verify that a credential is valid. Blockchain, which is an immutable data ledger, is generally used in digital ID projects as a key management tool rather than to store personal information. It contains public and private keys which act as a digital signature that the credential originates from a relying party.

2.4 DfE's education credential uses verified credential technology to enable learners to view and share their education record when applying and enrolling into FEIs. To support the education credential, DfE has created a digital wallet ('The Wallet App') that will be available to learners to download as an app from the Google Play App Store and Apple App Store. Learners will use the Wallet App to view and share their education record on their personal devices.

2.5 The aim of the education credential is to make the transition into further education easier for students and FEIs so that more time can be dedicated to helping learners get through the process rather than performing administrative tasks such as completing forms.

2.6 The ICO understands that there are three key data flows associated with the education credential as explained below:

- Credential issuance data flow
- Attainment data flow
- Application data flow

Credential issuance

2.7 Credential issuance is the process by which the credential for each learner is generated. Education credentials will be issued in person by members of staff in schools who know the learners and can verify they have received the correct education credential in a face-to-face setting. Members of staff will sign into DfE's 'Issue education records' service as a data issuer on a classroom computer. The staff member will be presented with a list of the learners in their school alongside their date of birth and Unique Learner Number (ULN). This information can be filtered into classroom groups. That member of staff will select a learner from the list. The selected learner will join the staff member in person with their mobile device, confirm that their identity matches the selected learner so that the staff member can proceed to issue the credential. This will generate a QR code on the member of staff's computer screen, which the learner can scan using DfE's Wallet App on their own mobile device. Learners will be presented with key information about what an education record is before being prompted to scan the QR code. If the learner chooses to scan the QR code, this will create an education record that they can view in the app on their phone. The education record contains information received from DfE by schools and exam bodies (see 2.10-12). DfE's education record app will be available for learners to download from both the Google Play Store (Android) and the Apple App store.

Attainment

2.8 The Attainment process describes how schools share a learner's information with awarding organisations (ie exam bodies) to facilitate their exam entry. Following this, awarding organisations send exam results to schools and to DfE where they are stored in the Learning Record Service (LRS). From the LRS, exam results are automatically made available in the learners' Wallet App as a verified education credential that learners can choose to share with FEIs for their enrolment processes. Learners can be alerted by push notification that their education credential has been updated with their exam results.

Application

2.9 The Application data flow consists of learners sharing the data from their digital wallet with FEIs. Learners will be able to use the app to share information from the credential directly with further education providers.

Personal information

2.10 The personal information that is processed within an education record includes:

- Name
- Unique Learner Number
- Date of birth
- Postcode
- Sex
- Next of kin/Emergency contact details
- Qualification details
- Schools attended
- Contact details (email/phone)
- National Insurance number

2.11 DfE will also be processing sensitive categories of data that form part of an education record such as free school meal entitlement. They will also be processing special category information such as Special Education Needs and health details.

2.12 Future developments of the credential may also process information that DfE holds about careers guidance activities that learners have undertaken.

3. Key data protection considerations

3.1 This section of the report provides a deep dive into each of the key data protection considerations for the development of DfE's education credential, and the work undertaken to address them in the Sandbox.

Lawful basis

3.2 Article 6 of the UK GDPR requires that a controller identify a valid lawful basis for processing in order to process personal information lawfully. Where that processing includes special category data, the controller must also identify an appropriate condition for processing under Article 9 of the UK GDPR (and where necessary, an appropriate condition set out in Schedule 1 of the Data Protection Act 2018 (DPA 2018)).

3.3 The education credential is intended to be more efficient than existing processes used to share information about pupils with FEIs. DfE needed support to determine whether the lawful basis for processing and condition for processing special category data that they use in existing processing would also be appropriate for the development of the education credential.

3.4 In order to assist with that assessment, the ICO sought to understand the application of the lawful basis to the existing processing that is used to share data about 16-18 year old learners with FEIs. DfE uses Article 6(1)(e) public task as the lawful basis for processing pupils' education records within the education system in England. In order for Article 6(1)(e) to apply, DfE's processing must be necessary for the organisation to perform a task in the public interest or for the organisation's official functions, and the task or function must have a clear basis in law. The processing must be necessary

and proportionate to carry out that task. DfE provided that the clear basis in law came from two existing legislative requirements for the provision of the LRS and Education and Skills Funding Agency (ESFA) 16-19 Funding as public tasks for which the education record would be necessary.

3.5 The relevant task for processing of learner data via the LRS is undertaken under Section 537A of the Education Act 1996, Provision of information about individual pupils, and Regulations made under Section 537A comprising the Education (Individual Pupil Information) (Prescribed Persons) Regulations 1999 and a series of amending regulations up to 2009 (the "Prescribed Persons Regulations").

3.6 This is supplemented by further applicable legislation, such as:

- Section 54 (Duty to give information) of the Further and Higher Education Act (1992)
- Regulation 5 (Provision of information by non-maintained special schools and Academies to the Secretary of State) of The Education (Information About Individual Pupils) (England) Regulations 2013

3.7 Provision of ESFA 16-19 funding is made under Section 14 of the Education Act 2002, (the) "Power of Secretary of State and National Assembly for Wales to give financial assistance for purposes related to education".

3.8 The processing includes special category data which is collected for the purpose of supporting any additional funding needs, any special adjustments that may be required, as well as statistical monitoring of the distribution of learners which is published and used for research purposes. DfE relies on the condition in Article 9(2)(g) of the UK GDPR - substantial public interest - for processing special category data. DfE has determined that the substantial public interest test in the first limb is provided by the processing allowing DfE and its executive agencies to ensure that the provision of education and children's services is effective and efficient, and the function being exercised is in the relevant legislation set out in relation to Article 6(1)(e) above. DfE finds that the second limb of paragraph 6 is satisfied by the exercise of DfE's functions as a central government department.

3.9 Having understood the lawfulness of DfE's existing process, the ICO used a comparative approach to determine whether the education credential involves substantially different processing, which could require a different lawful basis.

3.10 The ICO took the position that DfE can continue to rely on the existing Article 6(1)(e) of the UK GDPR - lawful basis 'public task'. Following discussion in the Objective one workshop, DfE was able to demonstrate that the verified credential collects the same personal information and seeks to achieve the same purpose as the existing processing. The ICO provided guidance that a determining feature is whether the credential is a more intrusive form of processing. Following this advice, DfE assessed that the new method is not more intrusive as no additional personal information is being processed or shared. The new processing activities would therefore be necessary and proportionate in the same manner as the existing processing activities.

3.11 As part of these considerations the ICO looked at the role of proportionality and found that, by streamlining the processing and giving learners more transparency over the data that is held within their Personal Learning Record, the new processing activities could be seen as an improvement to transparency and support the upholding of the public task as lawful basis.

3.12 Furthermore, as the verified credential aims to reduce the burden on both learners and providers during the enrolment process by providing a more secure way for learners to share enrolment information, DfE is acting within legislative requirements to promote education and exercising their powers with a view to improve standards, encourage diversity and increase opportunities for choice (Section 10 and Section 11 of the Education Act 1996). Implementing new technologies to improve how they exercise public tasks supports these legislative requirements. So long as these methods are proportionate, they would be unlikely to impact DfE's ability to apply the existing lawful basis to the deployment of the education credential.

3.13 DfE was therefore confident that they could continue to use the same lawful basis and condition of processing for the development of the education credential.

Controllership

3.14 One of DfE's objectives in the Sandbox was to establish where it was acting as a controller for each processing activity associated with the provision of the education credential. A controller determines the purposes and means of the processing, ie the 'why' and 'how' personal information will be processed. Other organisations such as schools and FEIs are also involved with the processing so it was necessary to determine the data protection roles for those parties too. Once established, all parties can take appropriate steps to adhere to their respective responsibilities under UK data protection law. Establishing the roles and responsibilities of all parties would also benefit learners who can directly access their education record via the Wallet App and should be able to understand the appropriate points of contact in respect of their record as well as their data protection rights.

The role of DfE

3.15 DfE entered the Sandbox with the view that they would be acting as a controller for the education credential. The ICO agreed with this view, noting that DfE determines the purpose of the credential and the public task that was identified as the lawful basis of processing. DfE also controls the means of how the credential will be used and managed, for example, DfE decides which categories of data will be available in the credential in the wallet. In addition, DfE has decided the technology that will be used to support the wallet and hosts the teacher-assisted site for the issuance of the credential. Namely, they have chosen to use a permissioned blockchain structure with managed access for specific actors such as schools and FEIs. DfE also processes the LRS from which data will be pushed into the wallet. These are clear examples of DfE exercising control over the means of processing that indicate that DfE is the controller for the credential.

The role of schools and Further Education Institutions (FEIs)

3.16 The ICO and DfE held a workshop to discuss the factors that indicate whether schools and FEIs act as separate independent controllers, or joint controllers, for personal information in the educational credential. As per Article 26(1) of the UK GDPR, where two or more controllers jointly determine the purposes and means of processing, they shall be considered joint

controllers. Controllers will not be joint controllers if they are processing the same data for different purposes in which case they will be separate independent controllers.

3.17 On application, although the activity benefits both schools and FEIs, neither party exercises sufficient control nor influence over the purposes and means of the development of the verified education credential jointly with DfE. As a result, schools and FEIs will likely not be joint controllers with DfE for this activity.

3.18 Schools collect much of the same data as DfE but do so for their own purposes found in the Education Act 1996 and they are under a statutory obligation to share information from their own records with DfE.

3.19 Similarly, FEIs will choose to collect information from the credential for enrolment purposes. This is a separate activity to the issuance and development of the education credential that is carried out by DfE. The purpose and means of the enrolment process are determined by the FEIs and therefore they are acting as an independent controller for this activity.

3.20 For the purposes of this report, it should be noted that while DfE's controller obligations were considered in detail, the obligations of other parties (ie schools and FEIs) were outside the scope of the Sandbox.

Role of learners and the wallet

3.21 The ICO and DfE discussed the implications of the learners holding their education record as a credential in a wallet app stored on their devices. Our view to DfE was that learners are data subjects in relation to the information held in the wallets. This is not affected by the fact that they are exercising control over their own data when choosing the FEIs with which they will share their information. DfE will remain a controller for the personal information held in the wallet as such information is sent from DfE's LRS database and is updated to reflect the information held by DfE.

3.22 As DFE is the controller for the issuance and management of the education credential, it is responsible for ensuring that processing complies with the UK GDPR.

Fulfilment of individual rights

3.23 As part of DfE's Sandbox plan, we agreed to look at how DfE could meet their obligation to fulfil individual rights throughout the credential process. In particular, we looked at the right to rectification and the right to erasure. We also looked at delegation i.e. where students with special needs may need to delegate access to these credentials to parents/carers.

3.24 DfE confirmed that they are not planning to create a functionality for individual rights from within the Wallet App but will instead signpost to the existing business-as-usual (BAU) process and privacy policy. DfE's existing BAU process for individual rights uses "contact us" forms with standard wording and is managed by a centralised data subject rights team. In particular, the Education and Skills Funding Agency (ESFA) has a BAU process that provides learners with a copy of their Personal Learning Record or allows them to raise a data challenge for correction as detailed in their online guidance. Where information is rectified, erased, or otherwise changed in the National Pupil Database (NPD) or Learning Record Service (LRS) it will automatically update in the corresponding issued verified educational credential. New credentials will be automatically pushed into learner wallets to replace the previous credential which has incorrect information or information that has now been deleted. Learners may receive an alert about the new credential via a push notification.

3.25 The ICO emphasised that it will be important to effectively signpost learners to the BAU process for delivering individual rights. The ICO advised DfE that it must be clear that the education credential forms part of the wider DfE system in regard to information that is held about the learner. The information should specify which organisation is best suited to deliver the learners' desired result. For example, where people are seeking to change information that can only be validated by a specific organisation and DfE will not be able to change it without that validation. Making sure that this information is transparent and suitable for the learners' age group was covered in Objective three of DfE's Sandbox plan and the outcomes of that work are discussed in the following section of this report.

Right to Rectification

3.26 During the workshop on individual rights, DfE indicated that different data categories held in the credential will be subject to different initiating points for the right to rectification. For example, where learners wish to have their examination results amended, they will need to go through the ESFA to raise a data challenge on their Personal Learning Record, following which the ESFA will investigate with the awarding organisation before the examination results are updated on DfE's systems and subsequently on the credential. However, where learners seek to add missing qualifications, they will need the school to raise a data challenge on their behalf through the Learning Record Service (LRS) organisational portal. Furthermore, where learners are seeking to rectify information related to Special Educational Needs or health assessments, they may need to rectify this information with the originating organisation of that information or directly with the relevant FEI when they are enrolled. DfE has a BAU process to rectify technical transposition errors such as misspelled names in the wallet and can issue a new educational credential to replace the inaccurate one.

3.27 The ICO advised DfE to map out the different types of rectification requests that learners could feasibly have and identify the different starting points of these requests as well as who will be needed to verify the accuracy of the information. Mapping out the different journeys will help DfE to take steps to provide effective transparency information that communicates to learners how they can exercise their rights in each case, particularly where information originates from organisations that learners are not likely to be aware of such as learning education authorities. This information will help to mitigate the risk that learners might seek to obtain changes to their information outside of the appropriate processes, for example where they are in dispute about an assessment of their educational needs.

3.28 Under Article 19 of the UK GDPR, if a controller has disclosed personal information that is subject to the right to rectification to other recipients, they must contact each recipient and inform them of the rectification of the personal information unless this proves impossible or involves disproportionate effort. In the context of the verified educational credential, this means that where DfE shares information from the credential with FEIs, DfE should have some means to inform these providers of changes to information after a rectification request. DfE should consider how FEIs that have received information will be informed when that information has been rectified. Given that learners have control over which FEIs receive their

information through the app, DfE should consider how learners can be given the necessary information to make it clear that they should inform providers that the information previously shared has been amended. The ICO recommended that DfE consider that where learners receive a push notification that their credential has been reissued following a rectification request, this could be a useful moment to encourage learners to reshare the rectified credential to the FEIs. This would make use of the fact that the wallet tells learners which recipient providers have received their information.

Right to Erasure

3.29 In the Sandbox, it was identified that there is a risk that learners who seek to delete or uninstall the credential app from their phone may do so on the basis that they believe that this action would completely delete the data when the information would remain on DfE systems (such as the NPD or LRS). It is important that DfE provides language that clearly explains the extent of the deletion function within the wallet. Specifically, the language should state in whose hands the information will remain after a learner seeks to delete the wallet from their device. The ICO suggested that DfE make that information available as learners uninstall the app. For example, DfE could make use of developer features to provide privacy and security information such as the data deletion section in Google App's data safety information, thereby making information accessible outside of the Wallet App. Learners will need to be directed to the BAU process for managing erasure requests to ensure they are made aware that this is distinct and a separate process from deleting the Wallet App.

3.30 During the Sandbox, DfE shared that the use of blockchain to deliver the education credential is not likely to affect DfE's ability to effectively erase information from the wallet as no personal information is to be stored on the blockchain, only DfE's public key. Instead, the verified education credential will use an audit database that records when a credential was issued and the payload of it which is stored in a secure relational database. The ICO advised DfE that it is important that those databases are added into the scope of individual rights such as the right to rectification and the right to erasure where it applies.

Delegation

3.31 In some instances, learners may need to delegate the sharing of information from the verified educational credentials to their guardian. To accommodate these needs, DfE has considered alternative issuance patterns such as using the guardian's email address so that support in the use of the credential can be carried out in the home. DfE is looking to use the Government Digital Service (GDS) OneLogin to establish guardian identity when accessing the credential at home. The proposed delegation process would break the issuance process (see 2.4) in two as the teacher would still verify the learner's identity and provide them with a pin code to create the credential at home rather than at school. The ICO advised DfE to carry out research with those guardians to see if such an alternative process is effective. This may need some input from schools as to how guardians for learners with support needs are typically involved in the existing enrolment and application process. DfE should also document how information about that process will be communicated to those who need it, including the role of the GOV.UK login and consider access for guardians who are not familiar with the GOV.UK login.

3.32 The ICO also highlighted that DfE should take steps to ensure that learners have authorised their guardians to manage their credential on their behalf. In particular, they should consider if there is a way to revoke guardian access to the credential should a learner decide that it is no longer necessary for that guardian to have access.

Interoperability

3.33 For the education credential, interoperability refers to the ability for all parties (schools, FEIs, learners) to exchange and use information from the education credential efficiently and without technical barriers. An interoperable credential can be issued by one party (DfE) to be verified and received by other organisations regardless of the technologies or standards they use. Verified credential typically use an open protocol which allows for interoperability. In the Sandbox, we considered the measures that DfE had taken to make the education credential interoperable so that learners from a variety of schools are able to share their education record with a wide range of FEIs with different technical capabilities.

3.34 Measures that DfE has taken to make the education credential interoperable include creating a detailed data specification that includes an English language version of specific codes so that the information in the education credential is both machine and human readable. DfE has shared this data specification with the main information management vendors that are used by FEIs. The ICO takes the view that these measures demonstrate good practice for interoperability as the information will be accessible to a wider range of FEIs who are not using standard machines to read the code and understand the input from the credentials.

3.35 DfE has identified three modes of interoperability to meet the varied technical capabilities of different providers and learners. The three levels of interoperability include:

- Verified credential;
- FEIs can use Application Programming Interfaces (APIs) to import an education record from the learners verified credential; and
- Use of account log ins (possible use of GOV.UK) as it allows learners who do not have access to a portable device to still obtain a verified credential.

3.36 Our feedback to DfE was that they should develop a review process for the effectiveness of the three modes of interoperability to evaluate how effective they are for resolving any technical barriers to the use of the education credential for specific groups of schools or FEIs.

3.37 In the workshop, DfE indicated that the data formats used across FEIs should be the same as the information received from the credential (ie according to census specification), and therefore this should not impact the ability of FEIs to input the information from the credential to their own systems.

Transparency (Articles 5(1)(a), 12 and 13 of the UK GDPR)

3.38 The UK GDPR requires controllers to be transparent with people about what they do with their personal information. DfE acknowledged that there were challenges in making sure that they provided information that learners aged 16 to 17 years

old could understand. In particular, there is a need to clarify that the credential is only part of the personal information that DfE processes about them. The Sandbox and DfE worked together to explore the communication strategies available to address these challenges and ensure that learners are informed about how their information is used throughout the education credential process.

3.39 In the workshop, DfE highlighted the difficulty in engaging learners who had not yet made an FEI application or gone through the enrolment process and therefore might struggle to understand the purpose of the education record credential. The ICO supported DfE's exploration of additional techniques such as mini videos of recent leavers talking about their experiences and how the education record app has helped them. The ICO suggested that these videos could include their thoughts about how their information is used. The ICO noted that DfE has extensive experience communicating with this age group and should make use of existing practice to consider the many ways they can provide transparency information. The ICO shared guidance on using the children's code principles. While these are not applicable to schools, they are useful criteria for DfE to consider as they are planning the pilots and seeking feedback on the privacy information to explore where improvements can be made. User testing will be fundamental here and looking at privacy information should be a specific part of the user testing.

3.40 DfE explained the user journey for learners on downloading the Wallet App for the credential. In the workshop, the ICO evaluated the appropriate touchpoints for providing transparency information in the user journey. DfE's position was to firstly explain what the education record is, how learners can use the record, and then allow learners to load the education record on the Wallet App using the QR code. These actions would take place before the learner is presented with the privacy notice summary. DfE was able to justify putting the privacy notice after the scanning of the QR code because their user testing showed that learners struggled to understand the privacy notice summary without viewing the information that it covered. The research also showed that providing the information in three brief screens stopped them scrolling without reading which they were more likely to do if the privacy notice was ahead of viewing their education record. The ICO was supportive of DfE's position given the use of user testing and research to consider the specific needs of their young audience when providing transparency information. In addition, learners are still able to decide not to proceed with using the wallet app upon reading the information. In regards to DfE's transparency obligations under Article 12 and 13 of the UK GDPR, the

information held in the education credential is data that has already been collected by DfE and subject to their personal information charter and DfE would also provide transparency information that schools could use with learners before they scanned the QR codes (see 3.43).

3.41 DfE's initial privacy notice summary linked to their centralised personal information charter which contains different privacy notices for the many data processing activities that DfE carries out. To help DfE fulfil their transparency obligations, the ICO recommended that, it would be more appropriate to link to something separate and user friendly for the target age group as it would be difficult for learners to identify the relevant notice for the education credential within the charter. DfE agreed that this would be useful and produced a draft version of this separate privacy notice for the ICO to review.

3.42 The ICO's main observation from the review was that the separate privacy notice was missing relevant privacy notice information about lawful basis and the DPO. The ICO acknowledged that it is fine to adopt a high level and layered approach to privacy information, and in fact this might be sensible to ensure learners are engaged based on DfE's user testing, however they must still ensure the notice is clear that it is a layer of available privacy information and be sure to signpost to the main privacy notice to provide all the information. DfE were advised to consider using technical capabilities to effectively signpost to the more detailed information in the personal information charter, for example linking directly to the DPO information and relevant lawful basis section so it is easier to navigate.

3.43 The ICO highlighted the role of schools in providing information about how the credential works at the point the teacher issues the credential. DfE has prepared a slide deck that schools can use to understand the process and explain it to learners, such as where the verifying information comes from. The workshop on transparency explored the various methods that schools used to explain the education credential such as assemblies, careers sessions, and PSHE which DfE had witnessed in the pilot. The ICO highlighted that providing schools with helpful guidance on explaining the process to learners would be essential to providing transparency given that DfE noted in the pilot that learners were able to understand the process most when it was explained by a teacher who they regularly interact with. DfE will be producing a range of materials including materials for senior leadership in schools, for those actually carrying out the process, for data administration and learners. DfE will test the materials as part of further pilots and give to schools to use as they prefer.

3.44 Whilst looking at the specific transparency challenges for the credential, the ICO raised the possibility that learners will likely be used to apps with preference centres where they can give and remove access in the app. To be transparent, DfE will need to provide clear messaging that, once information from the credential is shared with FEI providers, learners will not be able to remove that information from within the app and must manage access directly with the FEIs. As a result, DfE agreed that learners would benefit from a just-in-time notice being built into the user journey that would direct learners to FEIs after information has been shared.

3.45 DfE has also sought advice on how to be transparent as the education credential is only a part of the wider data landscape at DfE and therefore only part of the information that learners can retrieve in a subject access request. The ICO view in the Sandbox was that they should make sure that any transparency information they provide is clear about what the app covers and that it does not relate to any other information. The ICO offered that DfE could provide a brief signpost to the fact that schools and other institutions may hold other data about you. DfE provides learners with an example of an education record so they can see what information is contained in the education record which may help to mitigate the risk of misleading learners about the extent of the education credential. DfE were advised that should they start processing analytical information about how the education credential and Wallet App are used, they will need to amend their privacy notice to explain the purpose of that processing carried out by DfE.

Data protection risks

Security of processing (Article 32 of the UK GDPR)

3.46 As part of Objective four, the Sandbox and DfE worked on identifying data protection risks and their mitigations. In general, the information that DfE provided in the workshop suggested that the Wallet App is more secure and convenient compared to current methods that learners use to share their education record with FEIs, such as paper-based forms and in-person registrations.

3.47 During the workshop, the ICO drew attention to classroom-based risks during the issuance process such as other learners taking unauthorised pictures of the QR code to gain access to another learner's education record. In response, DfE confirmed that they had implemented a 'time to live' duration of five minutes for the QR code so that security risks such as unauthorised photos would be mitigated. The Sandbox was supportive of DfE's use of an additional step to "confirm this is you" where the learner's name and date of birth are displayed in-app prior to completing the onboarding which should reduce the chance of accidental access if the wrong QR code is presented. The ICO advised DfE that they should bolster these measures by offering support to schools to ensure consistency across the processes and procedures schools use to make sure QR code issuance is handled securely. An example could be the provision of prompts to engage simple protection steps.

3.48 The workshop also explored the necessary challenge between balancing security measures with usability for the target user group. DfE demonstrated a sensible approach to this balancing exercise and were encouraged to make sure that these considerations were properly documented in their data protection impact assessment (DPIA), referring to user testing and research when selecting the right security controls. Any residual risks should be acknowledged and signed off within the DPIA.

3.49 The Wallet App has been built using Google Firebase. Following a review of their security assessment documents, the ICO advised DfE to detail any customisations on the way the app is integrated and configured. This should include demonstrating that DfE has taken action to minimise the analytics data that is shared with Google and Firebase and whether DfE are applying default settings or not. The ICO's feedback to DfE highlighted that they should make sure they are asking for consent for non-essential analytics events as initially they had not identified that some app events were collecting the engagement_time_msec parameter which has the potential to be a very revealing metric; the parameter measures the amount of time that a user spends with the web page in focus or the app screen in the foreground. Google Analytics is collecting data on: if the user moves the app screen to the background, if the user focuses away from the webpage, if the user navigates away from the app screen or web page, or if the site or app crashes. This is measured in milliseconds as a number. Potentially, some learners (such as those with Special Educational Needs) may spend longer on an app or navigate differently revealing itself as a higher number which is sent to Google Analytics. The impact of this feedback was that DfE

carried out their own review to make sure non-essential communications in the Google Firebase pack were identified and would either not be sent or would seek consent. DfE were advised to develop this review by making sure the risks of collecting and sharing this information have been considered and the acceptance of these risks documented in the DPIA.

Purpose Limitation (Article 5(1)(b) of the UK GDPR)

3.50 Purpose Limitation as per Article 5(1)(b) of the UK GDPR requires that personal information be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes unless consent has been given, or it is required by law. This means that personal information from the education credential and Wallet App should be used in way that is in line with the reasonable expectations of learners based on the information provided (see section on Transparency).

3.51 Based on the discussion in the workshop, it is clear that discussions about prospective future uses for the credential are already taking place, with interest in additional functionality from both learners and government departments. DfE informed the ICO of the controls in place to manage function creep from the initial purpose of the credential. For example, DfE senior management participate in a steering group comprised of the directors of the Schools and Skills policy areas within DfE as well as external representatives. The steering group will have responsibility for reviewing suitable uses for the credential and ensuring that they align with the initial purpose of the processing. DfE will ensure that corporate governance is followed to manage changes. The ICO recommended that DfE should document the governance processes around the introduction of further purposes to make sure they are followed.

3.52 Where new uses for the education credential and the associated Wallet App are identified and no longer compatible with the initial processing, learners should continue to have the right to have their credential removed. DfE stated that new terms and conditions will be presented to learners, and the credential will be revoked if not agreed. If a credential is revoked, then that will disconnect the learner's device token from the credential. The ICO agreed that this should be implemented and considered with each new use.

Fairness

3.53 The ICO also noted that DfE needed to give further consideration to the impact to learners of not offering selective disclosure through the education credential as learners are only able to share the complete education record rather than specific categories. The ICO discussed the potential risk related to more sensitive data categories such as Special Educational Needs. DfE must demonstrate that the information that the credential shares is not more than is necessary to support learners' enrolment in an FEI and that they have done the analysis to support that view, this will also be relevant to their compliance with the data minimisation principle (Article 5(1)(c) UK GDPR). In the workshop, DfE stated that this information will always be requested by FEIs. Whilst FEIs usually require the information for enrolment and will always request it from learners, the credential may prevent learners being able to choose to not declare that information as they might have done in the pre-existing process even if that information would have eventually been requested by the FEI. In response, DfE confirmed that the pre-existing process for sharing information with FEIs will always be available as an alternative should learners wish to prevent some information being shared or if learners do not have access to a suitable mobile device.

4. Ending statement

4.1 DfE's participation in the Sandbox has been a useful exploration of the specific data protection challenges that controllers face when employing verified technology, including clarity on controllership and fulfilling individual rights especially within the unique context of the education system in England.

4.2 DfE welcomed the insight from the ICO, especially around simplified privacy notices, ensuring that all tracking usages are transparent and the rights to rectification processes are clearly laid out for their users in a way that is easy to understand and complete for these learners.

4.3 The Sandbox took place alongside a pilot that DfE carried out on a select group of schools which delivered useful insights and user testing opportunities that DfE has used to inform their approach to providing transparency information and support

to schools and FEIs. This demonstrates data protection by design in practice as DfE was able to adapt their approach using the advice received from the ICO.

4.4 The Department will be taking the pilot forward to ensure that the real-world identity assurance processes scale across hundreds of schools and to the further education organisations that will use the Education Credential. This is an example of how the ICO is supporting public sector organisations that are embracing the use of innovative technologies to deliver more efficient support.

4.5 DfE will now also be working closely with the software suppliers for the FE provider sector to ensure the seamless onwards flow of data enabled by this Education Credential is fully achieved.

4.6 Participation in the Sandbox has helped DfE to develop their education credential that makes processing more transparent for learners in a way that is secure. The ICO has provided DfE with regulatory certainty about the application of public task as a lawful basis when using innovative technologies. Going forward, DfE needs to consider how they will further apply the advice of the ICO to the next phase of rolling out the education credential this year.