Data Protection Impact Assessment Report

1)	A DPIA is a process designed to help you systematically analyse, identify, and minimise the data protection risks when deciding to process personal data. It is an essential part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all your data protection obligations.
2)	It does not have to eradicate all risk but should help you minimise and determine whether or not the level of risk is permissible and/or acceptable in the circumstances, taking into account the benefits of what you want to achieve.
3)	DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of activities e.g., policy, project, service delivery. Conducting a DPIA does not have to be complex or time-consuming in every case but there must be a level of rigour in proportion to the privacy risks arising.
4)	You should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an ongoing basis. You need to keep it under review and reassess if anything changes.
5)	DPIAs concern risks to individuals' interests. A DPIA must consider "risks to the rights and freedoms of natural persons". This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests, for example, material or non-material damage, significant economic or social disadvantage or prevention from exercising control over their personal data. The focus is therefore on any potential harm to individuals. The impact on society, as a whole, may also be a relevant risk factor. For example, it may be a significant risk if your intended processing leads to a loss of public trust.

DPIA Reference No.	
DfE/GDPR/2024-034	
Assessment of	
Technical consultation on a proposal for primary legislation to resolve issues in regard to the Department's financial powers	
Business Area	
Economic Vision	
Information Asset Owner	**Project Manager (if applicable)**
Giulia Ni Dhulchaointigh	Heidi-Beth Hudson

Proceed to Step 1 below.

STEP 1 DESCRIBE WHAT YOU ARE TRYING TO ACHIEVE
Describe the scope of what you are trying to do and include why you are doing it, your aims and objectives, and what types of processing it involves. Where applicable, it may be beneficial to refer or link to legislation, objectives, project Terms of Reference etc.
This is a consultation in relation to the Department for the Economy's (DfE) proposal for primary legislation to resolve issues in regard to some of the Department's financial powers. DfE has identified the following financial issues that it proposes to resolve via primary legislation: a. DfE's power to provide financial assistance where it is likely to be in the interest of the economy; b. DfE's power to exempt or remit certain fees in exceptional circumstances for Tourism Northern Ireland (TNI), for TNI to have the flexibility to introduce new fees where appropriate, and to extend TNI's existing ability to grade or classify certified tourist establishments to also include tourist amenities; c. DfE's power to form companies; d. Updating of section 1 of the Employment and Training Act (Northern Ireland) 19501; and e. the handling of smaller Departmental accounts (i.e. possible absorption within the main Departmental accounts).

STEP 2 DESCRIBE THE PROCESSING
Categories of data subject (for example, staff, students, children, vulnerable adults.)
Staff, other public sector organisations, voluntary/community/trade unions, others including - Private sector businesses, Industry, Local Councils, Academia & Educational Institutions (Universities, Colleges and Education Authorities).
Categories of personal data being collected (for example, contact details, financial data, educational attainment/qualifications, criminal convictions.) If creating a database/system that captures address details, consider the use of DoF's Pointer System.
Names, opinions, geographical location if provided, and contact email address. Additionally, we are seeking views on the draft section 75 and rural needs impact assessment as part of this consultation.

Is special category data (racial or ethnic origin, political opinions, religion, health, etc.) **or Criminal Offence data** (personal data about criminal allegations, proceedings or convictions) **involved?**
No special category or criminal offence data will be requested as part of the consultation.
What specific personal data is being collected within the category/categories of personal data? (Name, date of birth, home address, medical conditions, bank details, etc.)
Name, opinions, e-mail contact address, geographical location if provided, and where relevant, organisation. Supplying this information is optional – anonymous responses are allowed.
Who will provide you with the personal data? (This also includes providing the personal data to a data processor collecting the data on the Department's behalf)
The personal data will be provided by individuals responding on behalf of themselves, businesses, charities, or public bodies.
How will the personal data be collected/provided? (Where utilising online survey/consultation tools i.e. Citizen Space please click **here**. If using an external consultation tool, you need to be aware that Citizen Space was created due to the privacy risks of other tools.)
Survey data will be gathered in Citizen Space for eight weeks by respondents inputting their responses to the consultation questions. Responses will also be accepted during the consultation period, in email or written form, to the addresses provided in the consultation.
How will you store the data? (You should also include, if applicable, how a data processor will store the data on the Department's behalf.)
During the consultation period, responses made to the Citizen Space application will be stored in a secure file on the Citizen Space servers. Upon completion of the consultation, data will be transferred to a DfE Excel file, using a data transfer function in Citizen Space, and automatically deleted from Citizen Space. Written and email responses will be stored in secure folders in DfE's Content Manager document system. A dedicated mailbox has been set up allowing only authorised staff access and those with a legitimate interest in accessing the data. At the end of the consultation, they will be copied manually (typing or copy and pasting) to the Excel data file. After the copying process has been completed for all email/written responses, the Department will review each email/written response to ensure that it has been accurately transcribed. The Department will store the written and email responses in accordance with normal Departmental information and records management policies. The data will be stored in a password protected Excel file, in appropriately secured containers, in the Department's access-controlled Content Manager system. It will be retained in line with the Department's Retention and Disposal Schedule (R&DS).

Who will have access to the data? (Internally; includes if being held by a data processor.)
The Department's Financial Provisions Branch and selected other authorised DfE staff with a legitimate interest in accessing the data.
What will you do with the personal data once collected? (How will you use it?)
The Department will use the data provided in the responses to the consultation to inform the further development of the proposal for primary legislation to resolve issues in regard to the Department's financial powers. The Department may use the contact email addresses, if provided, to contact respondents where the Department considers that further information, or clarification of the response, would assist development of this legislative proposal. A summary of the responses provided will be published which will not include personal details, although may identify organisations that responded. The personal details will be held confidentially by DfE along with the full response.
Will you be linking the data to any other data held? (Data linkage involves connecting an individual person's information from at least two sources together for a specific purpose.)
No.
Will you in turn be sharing the data, for example, with another data controller, a data processor, or a third party? (If so, have you the appropriate documentation in place? e.g., contract, data sharing agreement, MoU. Where sharing personal data consider the use of SFTP/encryption.)
No. A summary of the responses will be published.
Will any decisions be made about the data without human intervention? (e.g., through the use of automated algorithms.)
No.
Scope of the processing
How long will it take to collect the information and how long will the data be processed (used)?
The consultation will run for a period of 8-weeks. It is anticipated that the data could be actively used for up to a period of 12 weeks following this time.

What will govern the length of time that the data will be retained for (once collected, created, etc.) and will this be included in the Department's Retention & Disposal Schedule? (Consider legislative, regulatory, industry standard, etc. to establish the retention timescale.)
The data will be retained for the duration of the development of the legislation and will be included in the Department's R&DS. In accordance with the Department's R&DS, the data will be retained for 5 years before being destroyed.
How many data subjects are likely to be affected and / or how many records involved? (Or an approximation where it is not possible to confirm precise numbers at present.)
It is estimated the number of responses will be between 10 and 30.
Where will the data be located after collection? (e.g., Content Manager, locked filing cabinets, storage devices, cloud-hosted services in UK, EU or international. This applies also to a data processor, where a data processor is involved, and should be recorded on the contract/MOU/ DSA.)
During the consultation period, data collected through the Citizen Space application will be stored in a secure file on the Citizen Space servers. Once the data has been transferred from Citizen Space it will be stored by DfE in appropriately controlled containers within DfE's document management system, Content Manager. Email responses and scanned copies of written submissions will also be stored here. Following being transferred to CM e-mails will be double deleted from the mailbox and hard copies will be shredded.
Will any of the personal or commercial data collected be made public or published? Why not, if it involves public money? (Grant Scheme beneficiaries, etc. (N.B. If it involves public money, it may be disclosable under FOI/EIR.))
No. A summary of the responses will be published but will not contain personal data. The respondents will not receive public money through responding to the consultation.
Context of the processing
Describe the nature of the relationship between the Department and the data subjects and how the relationship is established. (Contractual, to avail of a service, service delivery etc.)
The relationship will be established through the publication of the consultation documents, and the respondents' opportunity to make a response if wished.
Describe the extent to which the data subjects are aware of and expect their personal data to be used in connection with the proposed processing activities. (e.g., through a Privacy Notice at the time of collection or notification within a reasonable time frame.)
A link to the privacy notice for this consultation will be provided on the landing page of the consultation on the DfE website, and it will be referred to in the "How to respond" text of the consultation document.

Does the processing require the development of innovative technology? (If so, describe the level that current technology is at with regards to the processing being undertaken.)
No.
If using innovative technology or using existing technology in a novel way, including AI, describe the extent to which the processing activities are involved.
N/A.
Is the processing likely to raise any matters of public concern?
No.
Purposes of the processing
What do you want to achieve with this processing? (Describe the overall aims of the processing and how you have ensured it is legitimate.)
The Department's aim is to understand the views of respondents regarding the proposal for primary legislation.
What are the benefits to the data subject? (Describe how the processing benefits the data subjects/individuals either directly or indirectly and how you have ensured this processing is explicitly communicated to them at the time of collection.)
Processing data subjects' contact email addresses will benefit data subjects by ensuring that the Department can contact individuals or organisations interested in commenting on the Department's proposals and/or would like further information or clarification during the analysis of responses.
What are the benefits to the Department? (Describe how the processing benefits the Department either directly or indirectly.)
Processing will allow the Department to: • address any issues of concern which it had not previously identified. • follow up, or clarify, any responses, where appropriate; • increase public confidence in the final legislation.
What are the benefits to third parties? (Describe how the processing benefits any third parties either directly or indirectly.)
N/A
Are there any further purposes for which the information once held may be used for?
No.

STEP 3 CONSULTATION PROCESS

You should use the following boxes to fully detail the consultation process including (if appropriate) why consultation is not necessary.
Have you consulted all relevant internal stakeholders? (Data Protection Officer, Information Technology Security Officer (ITSO), DSO, other IAOs impacted upon? (N.B. If you are considering conducting an external survey, consider consulting Analytical Services/departmental NISRA representative.)) ***Please note: If you are using a digital solution you need to consult with the Departments ITSO.***
We have consulted the Department's IMU, DPO, Analytical Services, and IT Security Office.
Have you identified a high risk to data subjects that you cannot mitigate? (Article 36(1) requires consultation with the ICO when a DPIA has indicated that the processing would result in a high risk in the absence of measures taken to mitigate the risk. You cannot begin the processing until you have consulted them.)
There is no high risk to the data subjects.
Does your intention to process personal data stem from a new policy proposal captured in legislation? (Article 36(4) is a provision of GDPR which specifically imposes a requirement on UK Government to consult with the ICO.)
No.

STEP 4 DATA PROCESSORS
• **You should use the following boxes to fully detail if a data processor will be contracted to process data on behalf of the Department.** • **Processors act on behalf of the controller and under their authority. In doing so, they serve the controller's interests rather than their own.** • **Although a processor may make its own day-to-day operational decisions, it should only process personal data in line with a controller's instructions.** • **Refer to the ICO guidance on controllers and processors for further information.**
Are you using a data processor, and if so, have you been in consultation with them about requirements?
Delib, the company which develops and maintains the Citizen Space service, is the data processor. Citizen Space is the NICS recommended tool for online surveys. The CitizenSpace application has been Accredited for use in the NICS by the NICS Risk & Information Assurance Council and is considered suitable for processing of data marked up to OFFICIAL (including OFFICIAL-SENSITIVE). Accreditation is a formal process that looks at the application's security control & related procedures with the supplier & operating branch (NIDirect in this case) and whether they're appropriate for the intended use.
If using a data processor, is there a GDPR compliant contract in place?

(Further guidance is available at Data sharing - drafting contracts and agreements)
Yes - 1. Privacy Notice - NI Direct - Citizen Space 1. Citizen Space privacy statement - May 2020 PRIVACY STATEMENT (1).pdf (finance-ni.gov.uk) Citizen Space About - About - NI Direct - Citizen Space The GDPR compliant contract is managed by Digital Shared Services on behalf of the NICS. We have received confirmation that the Data Processor is GDPR Compliant
If using a data processor, detail the due diligence that has been performed? (GDPR requires this in relation to the data processor's implementation of appropriate technical and organisational measures.) Ensuring the adequacy of (third party) data processors
The GDPR compliant contract between Delib/Citizen Space and Digital Shared Services (on behalf of NICS) details the necessary technical and organisational measures which are required.
If using a data processor, detail how you will ensure compliance with what has been specified in the contract? (For example, if you have advised that the data processor must agree to an audit or return/destroy data at the end of the contract, etc.)
The DoF Digital Transformation team carry out twice yearly audits of the usernames that are processed by Delib - these usernames are related to DfE staff only in respect of this particular consultation. The GDPR compliant contract between Delib/Citizen Space and Digital Shared Services (on behalf of NICS) specifies how the data can be processed and stipulates that any processing beyond that agreed in the contract may be unlawful.
If allowing anyone other than staff to access data – especially if it is on DfE systems – have you considered the need for security clearance? (You may need to discuss with the Department's A/DSO to ascertain what is required.)
Processers will not be granted any access to DfE systems.

STEP 5 DATA CONTROLLERS AND JOINT DATA CONTROLLERS
You should fully detail if other data controllers, including joint data controllers, will have any relationship with the Department throughout this processing. (**Controllers** are the main decision makers – they exercise overall control over the purposes and means of processing personal data. If two or more controllers jointly determine the purposes and means of processing the same personal data, they are **joint controller**.)
Will you be sharing personal data with another data controller for example another public authority? (Detail here who this may be, if appropriate. Consider whether you may share data with authorities in the future, for example, NI Audit Office, another NICS Department, etc.)
No.

If sharing personal data with another data controller has a Data Sharing Agreement DSA been completed? (A DSA is **mandatory** in DfE in all cases where personal information is shared with another public authority.) Further information and guidance on drafting data sharing agreements can be found **Data sharing - drafting contracts and agreements** and **data sharing between controllers**.
N/A
Has a joint controller relationship been identified? (Detail here who this may be, if appropriate.)
N/A
Where a joint controller relationship has been identified, is there a transparent arrangement in place? (Joint controllers are not required to have a contract, but you must have a transparent arrangement that sets out your agreed roles and responsibilities for complying with the UK GDPR.)
N/A

STEP 6 ASSESS NECESSITY AND PROPORTIONALITY	
You should use the following boxes to fully detail the necessity and proportionality of the processing	
To lawfully process personal data you must identify a lawful basis under Article 6 of the GDPR: **Lawful bases for processing** (identify the most appropriate ground(s) for lawful processing, explaining the rationale).	The lawful basis for processing is that of public task in accordance with Section 8(d) of the Data Protection Act 2018 and Article 6(1)(e) of UK GDPR.
To lawfully process **Special Category data**, in addition to identifying a lawful basis under Article 6 of the GDPR, you must also identify a separate condition for processing under Article 9 and, where appropriate, the associated condition in UK law, set out in Part 1 of **Schedule 1 of the DPA 2018** (identify the most appropriate ground(s) for lawful processing, explaining the rationale).	N/A, no special category data will be processed.
To lawfully process personal data about **criminal convictions or offences**, in addition to having a lawful basis under Article 6, you must have either legal authority or official authority for the processing under Article 10	N/A, no personal data about criminal convictions or offences will be processed

and, where appropriate, the associated condition in UK law, set out in Part 1 of **Schedule 1 of the DPA 2018** (identify the most appropriate ground(s) for lawful processing, explaining the rationale).	
If processing special category data or criminal offence data, if required, has an Appropriate Policy Document (APD) been completed? Please provide the Content Manager record number of the APD.	N/A
Confirm this asset is recorded on the **Divisional Information Asset Register** and provide the Content Manager record number of your Divisional IAR to enable this to be verified.	EC1-24-2415
Necessity of processing (Is there another way to achieve the same outcome? Explain the extent to which the processing is necessary in relation to the purposes of the initiative).	The Department considers that there is no other practical and cost effective way to acquire public views on the proposal for primary legislation without public consultation and requesting public input.
Accuracy (describe the steps taken to ensure data quality in terms of accuracy both initially and on an ongoing basis).	All details will be provided by the respondent. Respondents enter their own data on Citizen Space, and transfer of data from Citizen Space to an Excel spreadsheet is via an automated transfer function within Citizen Space. Written and email responses will be provided by the respondent and then copied manually by DfE staff (typing or copy and pasting) to the Excel data file. After the copying process has been completed for all email/written responses, the Department will check each email/written response to ensure that it has been accurately transcribed.
Data minimisation **How will you prevent function creep?** (How will you safeguard data to ensure that it will not be used for any other purpose? Describe the steps that will be taken to ensure that the	The only personal data required is name, organisation (if relevant), geographical area (if relevant), views provided by the respondent and email contact details.

amount of personal data is adequate, relevant, and limited to what is strictly necessary both initially and on an ongoing basis.)	The data will only be used for the purposes detailed in this DPIA and in the consultation document. A summary report will be published without personal details but which may identify organisations that responded.
Fairness and transparency (describe the means by which data subjects will be informed about the intended processing, e.g., privacy notices).	A link to the Privacy Notice for this consultation will be included in the landing page for the survey on the DfE website.
Data subject rights (describe the steps taken to ensure that data subjects are able to exercise their rights fully and effectively, including the right to rectification in the event that data is inaccurate).	A link to the Privacy Notice will be included in the landing page of the survey on the DfE website and in the "How to respond" text of the consultation document. The notice will contain: • lawful basis for collecting data • how the data is collected and its purpose • who the data will be shared with • retention period • individual rights in respect of the processing • contact details for DPO and ICO to register complaints. The Privacy Notice will also detail the rights available to data subjects and who they may contact to exercise these rights. The introduction page will also provide the name and contact details of DfE and the official leading the survey project.
Storage limitation (describe the steps taken to ensure that personal data are not retained longer than necessary, in connection with the intended purposes of the processing, and this	Written and email responses will be copied manually (typing or copy and pasting) to a password protected Excel file in DfE's access-controlled Content Manager and will be retained in line with the Department's RD&S.

is reflected in the Department's Retention and Disposal Schedule).	After the copying process has been completed for all email/written responses, the Department will: 1 check each email/written response to ensure that it has been accurately transcribed; then 2 store email responses and scanned copies of responses in accordance with the Department's R&DS. For Citizen Space responses, the data is automatically transferred at the end of the consultation period, via the Citizen Space transfer function, to the consultation's Excel file in Content Manager and retained in line with the Department's RD&S. As part of the transfer process from Citizen Space to the Excel file, data will be immediately deleted from Citizen Space.
Security, integrity, and confidentiality (describe the steps taken to prevent the unauthorised and unlawful processing, accidental loss, destruction or damage of the personal data being processed).	Data will be treated as set out above for "Storage limitation", for security, integrity and confidentiality purposes. Data will not be shared with any other organisation.
Training (have all Departmental staff, involved with the data processing activity, completed mandatory data protection training?). Data Protection Essentials (NICS) Annual Training (see **LInKS**). NB: Training must be kept up to date i.e., refreshed annually.	Yes.
International transfers (identify any international transfers of personal data, whether or not to a third party processor, and	No international transfer of data.

the safeguards implemented in relation to such transfers).	

STEP 7 IDENTIFY AND ASSESS RISKS				
Ref No	**Describe source of risk and the potential impact on data subjects** (including associated compliance and corporate risks as necessary). Annex A contains details of the most common risks identified when processing personal data.	**Likelihood of harm** (Remote, Possible or Probable).	**Severity of harm** (Minimal, Significant or Severe).	**Overall risk** (Low, Medium or High).
	Example - The Department fails to meet the applicable rights of individuals, therefore in breach of UK GDPR and creating the potential for reputational damage and fines.	*Probable*	*Significant*	*Medium*
1.	Processing is not lawful, fair or transparent therefore in breach of UK GDPR and creating the potential for reputational damage and fines for the Department, and the unlawful processing of data subject's personal data and depriving of rights.	Remote	Severe	Low
2.	Processing takes place for an incompatible purpose resulting in a breach of the purpose limitation and accountability principle and a loss of public trust in how we use personal data.	Remote	Significant	Low
3.	Unnecessary data collection resulting in having more personal data than needed to achieve our purpose thereby being unlawful and in breach of the data minimisation principle.	Remote	Significant	Low
4.	Data held longer than necessary therefore potential to become irrelevant, excessive, inaccurate or out of date leading to unlawful processing. Data subject prevented from exercising control over their personal data.	Remote	Significant	Low
5.	Data not held securely therefore resulting in potential loss or abuse of personal data including identity fraud. Could lead to physical, material, and non-material damage.	Remote	Significant	Low
6.	Accountability principle not met in terms of appropriate technical and organisation measures therefore resulting in a loss of trust by data subject and possible enforcement action.	Remote	Significant	Low

7.	The Department fails to meet the applicable rights of individuals therefore in breach of UK GDPR and creating the potential for reputational damage and fines.	Remote	Significant	Low
8.	Privacy Notice does not adequately inform data subjects therefore Article 13 not met.	Remote	Significant	Low
9.	Data processors not UK GDPR compliant and arrangements not in place with partner organisations therefore obligations, responsibility and liabilities not documented.	Remote	Significant	Low
10.	Data processors handling data not aware of their responsibility to ensure staff are appropriately trained in relation to data protection therefore personal data mishandled resulting in reputational damage.	Remote	Significant	Low
11.	Lack of access to personal data held on system by DfE *(or delivery partners)* therefore resulting in the loss of availability and meeting the definition of a data breach.	Remote	Significant	Low

STEP 8 PROPOSED PRIVACY SOLUTIONS				
Ref No	**Measures to reduce or eliminate risks identified above. Consider what actions can be taken to address these identified risks.** (It is important to remember that the purpose of a DPIA is not to completely eliminate the impact on privacy but to reduce the impact to an acceptable level, while still allowing a useful project to be implemented.)	**Effect on risk** (Eliminated, Reduced or Accepted).	**Residual risk** (Low, Medium or High).	**Measure Approved?** (Yes/No)
	Example - Data subjects are informed of their rights in relation to being informed, of access, rectification, restricted processing, objection and be made aware of how to exercise their rights via the Privacy Notice provided. *System design and manual processes allow for access to personal data, should it be requested. Personal data rectified if it is inaccurate or incomplete, etc.*	*Reduced*	*Low*	*Yes*

1.	Processing will follow the guidance described in the UK GDPR compliant privacy notice and data protection impact assessment. All relevant rights under UK GDPR can be exercised.	Reduced	Low	Yes
2.	Data gathered by the survey will only be used to assist in the development of the proposed legislation as detailed in the privacy notice. The processing of contact email addresses is solely to invite further engagement with DfE. Respondents are only asked to provide contact details voluntarily should they wish the Department to engage further with them. The personal data will only be collected for specified, compatible purposes, and will not be used beyond these purposes unless truly anonymised.	Reduced	Low	Yes
3.	The Department is clear about what personal data is needed to achieve its purpose. Only the necessary amount of personal data will be collected.	Reduced	Low	Yes
4.	All data will be retained only for as long as necessary in line with the Department's Retention and Disposable Schedule.	Reduced	Low	Yes
5.	All data to be stored in a password protected Excel file within an appropriately controlled Content Manager container, in line with the Department's RD&S. Following transfer to Excel, data will be deleted from the external processor, Delib. Access to data limited to the Department's Economic Vision Directorate and specific authorised others with a legitimate need. No personal data is shared with other departments or third parties except as notified above.	Reduced	Low	Yes
6.	A Privacy Notice and a Data Protection Impact Assessment for this consultation have been completed to detail accountability for the collected personal data. The Department has ensured that those involved are aware of and adhere to their data protection responsibilities, has implemented proportionate policies and procedures, and is maintaining the necessary records of what is being done and why. Robust controls	Reduced	Low	Yes

	are in place to meet the requirements of the UK GDPR and appropriate reporting structures - recorded on Information Asset Register.			
7.	A link to the Privacy Notice for this consultation, confirming the rights of individuals will be included in the consultation landing page on the DfE website. This notice can be downloaded from the link. It provides contact details to permit citizens to exercise their data protection rights. System design and manual processes allow for access to personal data should it be requested; personal data rectified if it is notified as inaccurate or incomplete, etc.	Reduced	Low	Yes
8.	A link to the Privacy Notice for this consultation, confirming the rights of individuals will be included in the consultation webpage on the DfE website. The Privacy Notice can be downloaded from the link and viewed prior to providing any personal data.	Eliminated	Low	Yes
9.	The processor, Delib, is recommended for use by NICS. A GDPR compliant contract exists between Delib and Digital Shared Services (on behalf of NICS) which details the obligations, responsibility, and liabilities of the processor.	Eliminated	Low	Yes
10.	DfE colleagues processing the data have completed all necessary training and are aware of their responsibilities to correctly handle and store personal data. The external processer Delib has contractually agreed responsibilities with Digital Shared Services (on behalf of NICS).	Reduced	Low	Yes
11.	Recovery plans are in place to reduce the risk of loss of access occurring. Should this occur the data breach management plan will be followed.	Reduced	Low	Yes

STEP 9 APPROVAL PROCESS		
	Name/Date	**Notes**
Measures approved by:	**Heidi-Beth Hudson**	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If accepting any high residual risk, consult the ICO before going ahead.
DPO advice provided:	**Bernard McCaughan (pp)** **08/05/2024**	DPO should advise on compliance, Step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or not?		**If not, you must explain your reasons below.**
Comments:		
Consultation responses reviewed by:		**If your decision departs from individuals' views, you must explain your reasons below.**
Comments:		
This DPIA will be kept under review by:		**The IAO & DPO should review ongoing compliance with the DPIA.**

DOCUMENT CONTROL
The details of any reviews carried out should be captured in the table below, including reviews where no changes were necessary.

Review Date	Reviewer	Summary of changes	Approver	Approval date

Annex A

Potential GDPR risks and impact on data subjects	
1	Processing is not lawful, fair, or transparent; therefore, in breach of UK GDPR and creating the potential for reputational damage and fines.
2	Processing takes place for an incompatible purpose, resulting in a breach of the purpose limitation and accountability principle and a loss of public trust in how we use personal data.
3	Unnecessary data collection resulting in having more personal data than needed to achieve our purpose, thereby being unlawful and in breach of the data minimisation principle.
4	Inaccurate data could result in inaccurate decision making and mistrust with the data subjects involved.
5	Data held longer than necessary, therefore potential to become irrelevant, excessive, inaccurate, or out of date, leading to unlawful processing.
6	Data not held securely, therefore resulting in potential loss or abuse of personal data, including identity fraud.
7	Accountability principle not met in terms of appropriate technical and organisation measures, therefore resulting in a loss of trust by data subject and possible enforcement action.
8	The Department fails to meet the applicable rights of individuals, therefore in breach of UK GDPR and creating the potential for reputational damage and fines.
9	Data processors not GDPR compliant and arrangements not in place with partner organisations, therefore obligations, responsibility and liabilities not documented.
10	Data processors and joint controllers handling data, not aware of their responsibility to ensure staff are appropriately trained in relation to data protection, therefore personal data mishandled resulting in reputational damage.
11	Data re-matched due to improper anonymisation process of, therefore identifying or rendering identifiable data subjects.
12	Lack of access to personal data held on system by DfE *(or delivery partners),* therefore resulting in the loss of availability and meeting the definition of a data breach.