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/2024-035	
Assessment of	
Consultation on the Postgraduate Award Scheme	
Business Area	
Higher Education Research and Knowledge Exchange Branch	
Information Asset Owner	**Project Manager (if applicable)**
June Faccini	Johanne McCullough/Paul Murphy

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.

The Department for the Economy (DfE) is consulting on proposals to amend how the current DfE Postgraduate Award (PGA) Scheme is delivered including proposed changes to the Terms and Conditions.

DfE commissioned RSM UK Consulting LLP (RSM) to conduct a review of DfE's Postgraduate Award (PGA) scheme. The aim of the review was to evaluate the value for money and impact of the PGA Scheme to inform potential policy options going forward. This review was completed in 2023.

The consultation is open to the general public and seeks views from stakeholders and the general public regarding proposed options, discussed in the consultation document, to enhance and amend the current Postgraduate Award Scheme.

The consultation will include a privacy notice and the standard lines required in relation to FOI and data protection.

As part of the consultation process, when gathering responses, Higher Education Research and Knowledge Exchange Branch within the Department will process and log the following personal data in relation to respondents: Name; Postal/Email address; and Status/Category (i.e. individual/organisation/student/parent).

This data is collected to:

i. Allow a member of the Department to contact respondent via e-mail if further detail is needed to better understand the survey response, (if respondent has agreed to this approach)
ii. Allow the Department to share the results of the Consultation directly to those who have contributed to the consultation; and
iii. Allow the Department to analyse the views of respondents by category (see above).

Individual personal data of respondents will not be shared outside HE Research and Knowledge Exchange Branch. The container holding this data on the CM system will have restricted access to those officials managing the consultation only. Retention of this data will be in line with the Department's Retention and Disposal Schedule.

STEP 2 DESCRIBE THE PROCESSING

Categories of data subject (for example, staff, students, children, vulnerable adults.)

The consultation is open to the general public and requests the following categorisations: Individual; Organisation (likely to be a higher education institution or a students' union); or Student/parent.
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.
The consultation requests the following personal data within the "contact details" category: Name; Postal/Email address; and Status/category (i.e. whether they are a student/ parent /member of public/organisation). The opinions of the respondents will also be collected.
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
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.)
The consultation requests the following personal data within the "contact details" category: Name; Postal/Email address; and Status/category (i.e. whether they are a student/parent/ member of public/organisation).
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)
This personal data will be provided by either individuals responding in a personal capacity to the consultation, or individuals responding to the consultation on behalf of organisations.
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 by Citizen Space for two weeks. Upon completion of the survey, data held by Citizen Space will be transferred to a password protected Excel file within CM. A Consultation Response Form has been devised for this purpose. Respondents can either complete the form online through Citizen Space (an online tool) or submit a response directly to HE Research and Knowledge Exchange Branch via post. Information regarding how to respond is included in the consultation document.
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.)
Data will be deleted from Citizen Space when transferred to DfE. Excel data will be stored in appropriately secured Content Manager containers for as long as necessary to process in line with the Departments Retention and Disposal Schedule. The data will be stored in a restricted container on the Department's Content Manager system.
Who will have access to the data? (Internally; includes if being held by a data processor.)

The restricted container holding the data will only be accessed by those staff directly responsible for managing the consultation process – 1 Grade 7, 2x DPs and 1 SO.
What will you do with the personal data once collected? (How will you use it?)
The personal data will be used as follows: • Name and postal/email address – to allow the Department to respond directly to those who have contributed to the consultation; and Status/category – to allow the Department to analyse the views of respondents by category
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 – the data is for the purposes of the consultation only.
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.)
Whilst the data is for the purposes of the consultation only, information provided in response to the consultation, may be subject to publication or disclosure under access to information legislation (primarily the Data Protection Act 2018/the General Data Protection Regulations 2018 or FOI Act.
Will any decisions be made about the data without human intervention? (e.g., through the use of automated algorithms.)
No – the data is for the purposes of the consultation only; the team in HE Research & KE Branch responsible for managing the consultation will use the data as previously explained above.
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 be open for responses for a period of 8 weeks. Responses will be logged on a spreadsheet and saved into a restricted CM container upon receipt. Following closure of the consultation, responses will be analysed and a Departmental Response drafted and published. Personal data, such as names and email addresses, will not be published as part of this process. The status/category of respondents will be used to provide a picture of the scope of the responses to the consultation.
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.)
Retention of the responses to the consultation, including the personal data provided by the respondents, will be in line with the Department's Retention and Disposal Schedule (i.e. 5 years – policy development). The categorisation analysis of responses will be anonymised data, and

will also be subject to the Department's Retention and Disposal Schedule (i.e. 5 years – policy development).

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 difficult to provide a precise figure, as this is an open public consultation. A previous consultation on the Postgraduate Tuition Fee Loan received 180 responses however, a similar response rate is not anticipated for this consultation.

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.)

The data will be held in a restricted container on the Department's CM system.
Hard copy postal responses will log any postal responses onto the CM system and securely dispose of hard copy responses in confidential waste which is then 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 – the data is for the purposes of the consultation only.

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.)

This is a public consultation, published online, inviting responses from anyone who wishes to register their views on the subject matter (i.e. Options for Postgraduate Award Scheme). It is likely that respondents (i.e. data subjects) will fall into one of the following categories:

- Individual
- Organisation (likely to be a higher education institution or a students' union)
- Student
- Parent

Respondents can either complete the form online through Citizen Space or submit a response directly to HE Research and KE Branch via post. Information regarding how to respond is included in the consultation document. The Department will ensure each respondent receives a copy of the Departmental Response to the consultation at the end of the process.

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.)

At the time of publication of the consultation, the Department will include a Privacy Notice which advises respondents of the nature of the data requested and how the Department will process/ manage that data.

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 - the data is for the purposes of the consultation only.
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 - the data is for the purposes of the consultation only.
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 for the Economy is responsible for the policy in relation to the Postgraduate Award Scheme; this consultation process is necessary before any amendments to this policy may be introduced. Personal data collected in this consultation exercise will be used for analysis and reporting of consultation responses under the lawful basis of public task in line with the Data Protection Act 2018 and the General Data Protection Regulations 2018. The Department for the Economy is consulting on proposals to amend the current Postgraduate Award Scheme. The consultation is open to the general public and seeks views from stakeholders and the general public regarding proposed options, discussed in the consultation document, to enhance and amend the current Postgraduate Award Scheme.
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.)
The feedback and views provided by the data subjects in their responses to the consultation will be used when considering amendments and improvements to the current policy in relation to the Postgraduate Award Scheme. This will ensure that all respondent views are considered fully and the Department will provide justification, if applicable, where a particular viewpoint cannot be accommodated. Collecting the contact data will ensure the Department can issue the Departmental Response to the consultation to each individual respondent.
What are the benefits to the Department? (Describe how the processing benefits the Department either directly or indirectly.)
The consultation process allows the Department to ensure that the views of those who may have an interest in the policy area are gathered, analysed and considered when making amendments to/improving the policy. Collecting the contact data allows the Department to issue the Departmental Response to the consultation to each individual respondent and to analyse the categories of respondent.
What are the benefits to third parties? (Describe how the processing benefits any third parties either directly or indirectly.)

The consultation process allows the Department to ensure that the views of those who may have an interest in the policy area are gathered, analysed and considered when making amendments to/improving the policy. This will benefit others who may not have responded to the consultation. The collection of the contact data will have no impact on third parties.
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.***
ITSO has been consulted re. the use of Citizen Space for the consultation. DPO has been consulted as part of the DPIA process.
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.)
No
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 HERE for further information.**
Are you using a data processor, and if so, have you been in consultation with them about requirements?

Yes, Citizen Space. 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.)
No further security clearance required. Only a small number of DfE staff in the policy team conducting the consultation will have access.

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 here and here.
N/A
Has a joint controller relationship been identified? (Detail here who this may be, if appropriate.)
No
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.)
No

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).	Public task - The Education (Student Support) (Northern Ireland) Order 1998 makes provision for the Department to make grants or loans to eligible students in connection with their attending higher education. The Department is responsible for the policy in relation to the Postgraduate Award Scheme. The Department is seeking views, through a public consultation, on proposals to amend the current policy.
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	N/A

of **Schedule 1 of the DPA 2018** (identify the most appropriate ground(s) for lawful processing, explaining the rationale).	
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 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
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.	As recorded within HE Divisional IAR EC1/23/0431328
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).	Without collecting the contact details of respondents to the consultation, the Department cannot ensure that each respondent subsequently receives a copy of the Departmental Response or contact the respondent for further information if they have indicated that they agree to this approach. Without collecting details of the status/category of respondents to the consultation, the Department cannot analyse the scope of respondents and the impacts of any policy changes on certain categories.
Accuracy (describe the steps taken to ensure data quality in terms of accuracy both initially and on an ongoing basis).	Information is provided directly by respondents to the consultation. This will be stored in the same format on the Departmental CM system and logged on a spreadsheet. All will be subject to restricted access, including those received by hard copy until they are stored in CM and then disposed of securely.

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 amount of personal data is adequate, relevant, and limited to what is strictly necessary both initially and on an ongoing basis.)	Only the personal data (including opinions) required to complete this task will be collected. The personal contact data (name and postal/email address) will be collected and held for the sole purpose of issuing a Departmental Response to each respondent or contacting them to discuss their response (if they have indicated they agree to this approach) .
Fairness and transparency (describe the means by which data subjects will be informed about the intended processing, e.g., privacy notices).	At the time of publication of the consultation, the Department will include a Privacy Notice which advises respondents of the nature of the data requested and how the Department will process/manage that data.
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).	The Privacy Notice includes all necessary information. In addition, the consultation response form advises that personal data will not be published or shared with any third parties.
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 is reflected in the Department's Retention and Disposal Schedule).	Retention of the CM records will be in line with the Departmental Retention and Disposal Schedule (5 years). The categorisation analysis of responses will be anonymised data, and will also be subject to the Department's Retention and Disposal Schedule (i.e. 5 years – policy development).
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).	Hardcopy postal responses will be logged onto the CM system and the hard copy disposed in confidential waste then shredded. The information provided will be retained in a restricted container on the Departmental CM system. Access will be restricted to the team responsible for undertaking the consultation – 1 Grade 7, 2x DPs and 1 SO.
Training (have all Departmental staff, involved with the data processing activity, completed mandatory data protection training?). Data Protection Essentials (NICS) Annual Training (see **LInKS**).	Yes.

NB: Training must be kept up to date i.e., refreshed annually.	
International transfers (identify any international transfers of personal data, whether or not to a third party processor, and the safeguards implemented in relation to such transfers).	N/A

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	Remote	Severe	Medium
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	Medium
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	Medium
4.	Data held longer than necessary therefore potential to become irrelevant, excessive, inaccurate or out of date leading to unlawful processing.	Remote	Severe	Medium
5.	Data not held securely therefore resulting in potential loss or abuse of personal data including identity fraud.	Remote	Significant	Medium
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	Medium
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	Medium
8.	Privacy Notice does not adequately inform data subjects therefore Article 13 not met.	Possible	Significant	Medium

9.	Data processors not GDPR compliant and arrangements not in place with partner organisations therefore obligations, responsibility and liabilities not documented.	Possible	Significant	Medium
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.	Possible	Significant	Medium
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.	Possible	Significant	Medium

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 GDPR compliant privacy notice and data protection impact assessment. All relevant rights under GDPR can be exercised.	Reduced	Low	Yes
2.	Data gathered by the survey will only be used to assist in considering the options for the PGA Scheme as detailed in the privacy notice. The processing of contact email addresses is for the purpose of issuing a Departmental Response to each respondent	Reduced	Low	Yes

	and contacting the respondent to discuss their opinion, if they have indicated they agree to this approach . The personal data will only be collected for specified or compatible purposes and will not be used beyond these purposes unless truly anonymised.			
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 only be retained for as long as necessary in line with the Departments Retention and Disposable Schedule.	Reduced	Low	Yes
5.	All data to be stored in a password protected Excel file within Content Manager, in line with the Departments Retention and Disposable Schedule. Following transfer to excel, data will be deleted from the external processor, Delib.	Reduced	Medium	Yes
6.	A privacy notice and data protection impact assessment has 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 in place to meet the requirements of the UK GDPR and appropriate reporting structures - recorded on Information Asset Register.	Reduced	Low	Yes
7.	A privacy notice confirms the rights of individuals. This notice can be downloaded from the surveys landing page and provides contact details to permit citizens to exercise their rights. System design and manual processes allow for access to personal data should it be requested; personal data rectified if it inaccurate or incomplete, etc.	Reduced	Low	Yes
8.	A privacy notice has been drafted. This notice can be downloaded from the surveys landing page 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:	**June Faccini – 15/04/2024**	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:	**June Faccini – 15/04/2024**	If accepting any high residual risk, consult the ICO before going ahead.
DPO advice provided:	**Bernard McCaughan (pp)** **19/04/2024**	DPO should advise on compliance, Step 6 measures and whether processing can proceed.
Summary of DPO advice: Please see comment in Step 2, page 4 and address accordingly.		
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:	**June Faccini**	**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.