

DE DATA PROTECTION IMPACT ASSESSMENT SCREENING EXERCISE

Please read chapter 4 of DE Conducting a Data Protection Impact Assessment guidance before completing this exercise – available in IMT section on DE Intranet:

<http://nics.intranet.nigov.net/education/documents/general-data-protection-regulation-2016-and-data-protection-act-2018-gdprdpa>

Project Name:
Temporary Variation (TV) Policy Review Consultation Survey

Directorate:
**Sustainable Schools Policy and
Planning Directorate**

Team:
School Admissions Team

1. PROJECT SUMMARY

The survey is in relation to a review of the Temporary Variation (TV) Policy. When a school is oversubscribed with applications, it may apply to the Department to admit additional, named children. TV Policy (Circular 2026/03), provides the existing framework for how requests for additional places are considered, including the criteria and safeguards that apply. Under the current framework, decisions have primarily been based on availability within a school sector rather than preference for a specific school.

Recent admissions data indicates that parental preference is often driven by a desire for a particular school rather than by school sector. This has highlighted a potential mismatch between how the system operates and how parents make choices

To inform the review of TV Policy, a consultation process constituting an online survey, which may be responded to in hard copy if preferred, is being used.

2. STAKEHOLDERS

We are asking the following stakeholders to complete the survey regarding the Temporary Variation Policy Review Survey:

The consultation will be issued to every primary and post-primary Board of Governors inviting them and the wider school community to provide responses. The consultation will also be issued to the various sectoral bodies for their consideration. The consultation will be published on the Department of Education website and responses will be welcome from anybody including:

- School governors
- Teachers
- Educational Practitioners
- School leaders
- Parents or guardians
- Any member of the public

3. BRIEF DESCRIPTION OF PERSONAL DATA INVOLVED

The survey does not request name, address, email, date of birth, phone number etc. It does request what stakeholder group the respondent belongs to and what phase of education they are involved in along with their views on a number of questions.

We do not request any information that could identify a person.

4. PRIVACY ASSESSMENT

Use this checklist to assess the project for privacy risks. The questions below will help you consider whether a DPIA is necessary.

(i) Does the project/activity involve any of the following high risk processing	Yes	No	If yes, explain your response
Systematic or extensive profiling, evaluation or scoring	☐	☒	(Insert text)
Large scale processing of sensitive data	☐	☒	
Systematic monitoring of individuals	☐	☒	
Use of new technology or novel use of existing technology (e.g. AI)	☒	☐	We plan to use M365 Copilot to help analyse the responses.
Denial of individuals' access to a service	☐	☒	
Profiling of individuals on a large scale	☐	☒	
Processing of biometric data	☐	☒	
Processing of genetic data	☐	☒	
Processing of sensitive data or data of a highly personal nature	☐	☒	
Combining, comparing or matching data obtained from multiple sources	☐	☒	

Invisible processing	☐	☒	(Insert text)
Tracking geolocation or behaviour	☐	☒	
Targeting of children or other vulnerable individuals	☐	☒	
Risk of physical harm	☐	☒	

If you answer yes to any of the questions in section 4(i) above, it is likely that a DPIA will be automatically required. Consult to DE Data Protection Officer for further advice.

(ii) Does the project involve any of the following?	Yes	No	If yes, explain your response
Automated decision-making with a legal or similar significant effect.	☐	☒	
Processing of data on a large scale.	☐	☒	
A change to an existing policy, process or system that involves personal data (e.g. new legislation or policy that makes it compulsory to collect or disclose information).	☐	☒	
A change in location of a business area or branch (e.g. plans to centralise a service or an office move).	☐	☒	
A practice or activity that is listed on a risk register (e.g. activities listed on your business area's risk register or health and safety register).	☐	☒	
Collecting new information about an individual (e.g. gathering information about individuals' location).	☐	☒	
A new way of gathering personal information (e.g. collecting information online rather than on paper forms).	☐	☒	
A change in the way personal information is stored or secured (e.g. cloud storage).	☐	☒	

A change to how sensitive personal information is managed (e.g. moving health records to a new database).	☐	☒	<i>(Insert text)</i>
Transferring personal information offshore (e.g. using a cloud based application to store data).		☒	<i>(Insert text)</i>
A decision to retain personal information for longer than previously kept (e.g. keeping information for 10 years when you previously only held it for 7).	☐	☒	
Using information classed as 'special category data' (e.g. information about an individual's health).	☐	☒	
Using personal data already held for a new purpose (e.g. to obtain customer profiles).	☐	☒	
Disclosing information to a third party (e.g. following a request from a law enforcement agency to provide information for a particular purpose).	☐	☒	
Sharing or matching personal information held by different organisations or in different datasets (e.g. combining data with other information held on systems or sharing information to enable organisations to provide services jointly).	☐	☒	
A change in policy that results in people having less access to information that you hold about them (for example, archiving documents after 6 months into a facility from which they cannot be easily retrieved).	☐	☒	
Establishing a new way of identifying individuals (for example, a unique identifier, a biometric, or online identity system).	☐	☒	

Introducing a new system for searching individuals' property, persons or premises (e.g. adopting a new policy of searching data on mobile phones that have been returned for upgrading).	☐	☒	(Insert text)
Surveillance, tracking or monitoring of movements, behaviour or communications (e.g. installing a new CCTV system or monitoring a member of staff's email account).	☐	☒	(Insert text)
Changes to premises impacting on private spaces where clients/staff may discuss personal data (e.g. changing the location of a reception desk where people may disclose personal details or relocating a branch where sensitive personal data is processed).	☐	☒	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them (e.g. <i>adding a new medical condition to the requirements of a licence.</i>	☐	☒	
Other privacy intrusions such as body searches, or intrusion into physical space.	☐	☒	

Additional Comments/Notes

5. INITIAL RISK ASSESSMENT

If you answered 'Yes' to any of the questions in section 4, use the table below to give a rating - either Low (L), Medium (M), or High (H) – to each of the aspects of the project set out in the first column. If you answered 'No' to all the questions in section 4, move on to section 6.

Aspect of the Project	Rating (L, M or H)	
Level of personal data handling	L – Minimal personal information will be handled	☒
	M – A moderate amount of personal information (or information that could become personal information) will be handled	☐
	H – A significant amount of personal information (or information that could become personal information) will be handled	☐
Sensitivity of information	L – The information is not sensitive	☒
	M – The information may be considered to be, or may become, sensitive	☐
	H – The information is highly sensitive	☐
Significance of the changes	L – Only minor change to existing functions/activities	☒
	M – Substantial change to existing functions/activities; or a new initiative	☐
	H – Major overhaul of existing functions/activities; or a new initiative that's significantly different	☐
Interaction with third parties	L – No interaction with other agencies	☒
	M – Interaction with one or two other agencies	☐
	H – Extensive cross-agency (government) interaction or cross-sectional (non-government and government) interaction	☐
Public impact	L – Minimal impact on the organisation and individuals	☒
	M – Some impact on individuals is likely due to changes to the handling of personal information; or the changes may raise public concern	☐
	H – High impact on individuals and the wider public; concerns over aspects of project or negative media interest is likely.	☐

6. SUMMARY OF PRIVACY IMPACT

The privacy impact for this project has been assessed as:

Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm



6. SUMMARY OF PRIVACY IMPACT

eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated.	
Medium* – Some personal information is involved, and several low to medium risks have been identified	☐
High* – Sensitive personal information is involved, and several medium to high risks have been identified	☐
Reduced risk – The project will lessen existing privacy risks	☐
Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.	☐
Briefly summarise reasons for the rating given: We do not request any information that could identify a person. Some of the questions have free text boxes, in light of any potential data protection issues arising and to prevent the possibility of someone including personal information we have stated 'Please do not include any personal data in your response' at each free text box. M365 copilot operates with our own Microsoft 365 environment, using data I already have access to. All prompts, responses and user content stay within the tenant and are not shared with Microsoft. Copilot can only access data that I already have access to via Microsoft Graph. Copilot will not make any automated decisions, and all output will be fact checked.	

* If you have assessed the privacy impact as medium or high, a DPIA must be carried out.

7. RECOMMENDATION

A full data protection impact assessment **is** required

☐

A full data protection impact assessment **is not** required

☒

Reasons:

We are not requesting any information that could identify a person. Copilot will not make any automated decisions, all output will be fact checked. Copilot makes use of Enterprise Data Protection, which is the same protection offered by Microsoft for emails

8. SIGN OFF

Project Manager

Name:
Joyce Nickell

Date:31 July 26

Signed:



Senior Responsible Owner/Information Asset Owner

Name:
Craig Boyd

Date:31 July 26

Signed:

