DATA SHARING AGREEMENT

Between

the Department of Education
and
the Educational Research Centre

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

Conducting independent research on all aspects of education and at all levels of the education system including educational research that will inform policy making and the improvement of educational standards.

Table of Contents

Interpretation Table 3
Data Sharing Agreement 4
1. Evaluation for a Data Protection Impact Assessment (DPIA) 5
2. Purpose of the Data Sharing 7
3. Data to be shared 12
4. Function of the Parties 14
5. Legal Basis 17
6. Impetus for Data Sharing 19
7. Categories of Data Shared 20
8. Duration and Frequency 21
9. How data will be processed 22
10. Restrictions 24
11. Security Measures 25
12. Retention 33
13. Methods Used to Destroy/Delete Data 34
14. Withdrawal from Agreement 35
15. Other Matters 36
16. Schedule A - Data Protection Impact Assessment 38
17. Schedule B 40
18. Schedule C 42
19. Authorised Signatory 43
Data Protection Officers Statement 44

Interpretation Table

DEFINITION	MEANING
Data controller	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Party disclosing data	Shall mean the Party transferring personal data to the receiving Party or Parties.
Party receiving data	Shall mean the Party receiving personal data from the Party disclosing data.
Data Protection Impact Assessment(DPIA)	Means an assessment carried out for the purposes of Article 35 of the General Data Protection Regulation.
GDPR	Shall be taken as a reference to the General Data Protection Regulation (2016/679) including such related legislation as may be enacted by the Houses of the Oireachtas.
Lead Agency	Refers to the Party to this agreement who is responsible for carrying out the functions set out in 18(2), 18(3), 21(3), 21(5), 22(1), 55(3), 56(1), 56(2), 57(4), 58, 60(1) and 60(4) of the Data Sharing and Governance Act 2019.
Personal Data	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Personal data breach	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Processing	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Public Service Body (PSB)	Means a Public Body as defined by section 10 of the Data Sharing and Governance Act 2019.
Shared personal data	Means data shared pursuant to this agreement.

Table 1.0

Data Sharing Agreement

BETWEEN

Insert name of Lead Agency, having its registered address at:

LEAD AGENCY NAME	ADDRESS
The Department of Education (DE)	Marlborough Street, Dublin 1 D01 RC96

AND

Insert name(s) of Other Party/Parties to the agreement, having its registered address at:

PARTY NAME	ADDRESS
The Educational Research Centre (ERC)	DCU, St. Patrick's Campus Drumcondra Road Upper Dublin 9 D09 AN2F

The Parties hereby agree that the Department of Education will take the role of Lead Agency for the purpose of this Data Sharing Agreement.

Each of the Parties to this agreement are data controllers in their own right when processing personal data on their own behalf, for their own purposes.

1. Evaluation for a Data Protection Impact Assessment (DPIA)

The completion of a DPIA can help data controllers to meet their obligations in relation to data protection law. Article 35 of the GDPR sets out when a DPIA is required.

Data controllers should periodically re-evaluate the risk associated with existing processing activities to understand if a DPIA is now required.

1.1 Identifying if a DPIA is required

The below checklist can assist organisations to understand if they require a DPIA pursuant to Article 35 GDPR to support their data sharing agreement. The questions should be answered in relation to the entire project that the data share corresponds to. This ensures that Public Service Bodies (PSBs) have the opportunity to be transparent in the evaluation of risks in relation to the data required for this process.

The completion of a DPIA is relevant to this data sharing agreement as you will be asked to provide a summary of any DPIA carried out in Section 16 of this document.

The questions below should be completed by the Lead Agency together with the Other Parties involved in this data sharing agreement. Please contact your DPO in relation to the requirement to carry out a DPIA.

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.1	Processing being carried out prior to 25th May 2018?	YES

Table 1.1

If **'Yes'** proceed to 1.2
If **'No'** proceed to 1.1.2

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.2	A new purpose for which personal data is processed?	NO
1.1.3	The introduction of new types of technology?	NO

Table 1.2

If '**Yes**' to either of the last two questions, proceed to 1.1.4.
If '**No**' to both of the last two questions, proceed to 1.2.

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.4	Processing that is likely to result in a high risk to the rights and freedoms of natural persons?	NO

Table 1.3

If '**Yes**', then you are likely required to carry out a DPIA under Article 35 GDPR.
If '**No**' proceed to 1.2.

1.2 Further Considerations

There are limited circumstances where a mandatory DPIA should be carried out, even where processing was underway prior to the GDPR coming into effect[1].

	DOES THE PROCESS INVOLVE:	YES/NO
1.2.1	A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning individuals or similarly significantly affect individuals.	NO
1.2.2	A systematic monitoring of a publicly accessible area on a large scale.	NO
1.2.3	The Data Protection Commission has determined that a DPIA will also be mandatory for the following types of processing operation where a documented screening or preliminary risk assessment indicates that the processing operation is likely to result in a high risk to the rights and freedoms of individuals pursuant to GDPR Article 35(1): Lists of Types of Data Processing Operations which require a DPIA. (*if this hyperlink does not work, use the following url: https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf*)	NO

Table 1.4

If **'Yes'** to any then you are likely required to carry out a DPIA under Article 35 GDPR.

If **'No'**, to all then a DPIA may not be required.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

2. Purpose of the Data Sharing

2.1 Framework

This Data Sharing Agreement sets out the framework for the sharing of personal data between the Parties and defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to one another.

This agreement is required to ensure that any sharing of personal data is carried out in accordance with the GDPR and the Data Sharing and Governance Act 2019, and each Party agrees to be bound by this agreement until such time as the agreement is terminated, or the Party withdraws from the agreement.

The Parties shall not process shared personal data in a way that is incompatible with the relevant purposes and this agreement.

The Parties will ensure that the Data Sharing Agreement remains fit for purpose, accurate and up to date.

The Parties will actively monitor and periodically review the data sharing arrangement to ensure that it continues to be compliant with data protection law, that it continues to meet its objective, that safeguards continue to match any risks posed, that records are accurate and up to date, that there is adherence to the data retention period agreed and that an appropriate level of data security is maintained.

The Parties must address all recommendations made regarding this Data Sharing Agreement by the Data Governance Board.

2.2 Performance of a Function

Where a public body discloses personal data to another public body under this agreement, it shall be for the purpose of the performance of a function of the public bodies mentioned, and for one or more of the following purposes (please select):

No.	DESCRIPTION	Select
I	To verify the identity of a person, where one or more of the public bodies are providing or proposing to provide a service to that person	☐
II	To identify and correct erroneous information held by one or more of the public bodies mentioned	☐
III	To avoid the financial or administrative burden that would otherwise be imposed on a person to whom a service is being or is to be delivered by one or more of the public bodies mentioned where one of mentioned public bodies to collect the personal data directly from that person	☐
IV	To establish the entitlement of a person to the provision of a service being delivered by one or more of the public bodies mentioned, on the basis of information previously provided by that person to one or more of the public bodies mentioned (or another public body that previously disclosed the information to one or more of the public bodies mentioned)	☐
V	To facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	☒
VI	To facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	☒
VII	To enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	☒
VIII	To facilitate an analysis of the structure, functions, resources and service delivery methods of one or more of the public bodies mentioned	☒

Table 2.2

2.3 Details about the Purpose

Provide details of the particular purpose of this Data Sharing Agreement.

PURPOSE	DESCRIPTION
V - To facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned. VI - To facilitate the improvement or targeting of a service,	The personal data of students is collected by their school for the purpose of providing education and fulfilling the functions of a recognised school under the Education Act 1998 as amended, one of these functions being to maintain systems whereby the efficiency and effectiveness of its operations can be assessed, including the attainment levels and academic standards of students (section 9(k) of the Act). Certain types of special category personal data are collected and processed under the legal basis of consent. Only aggregated special category personal data (as outlined in section 3.4 of the DSA) are shared by the Department with the ERC under this DSA. The school provides student personal data to the Department. The legal bases for this sharing and collection by the Department are the Education Act, the Social Welfare Consolidation Act 2005, the Education Welfare Act 2000 and SI 317 of 2015 (Social

programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned VII - To enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned VIII- To facilitate an analysis of the structure, functions, resources and service delivery methods of one or more of the public bodies mentioned	Welfare (Consolidated Claims, Payments and Control) (Amendment) (No. 4) (Sharing of Information) Regulations 2015). The data of students in participating schools as set out in this agreement is then shared by the Department with the ERC. Parents/guardians are informed that pupil data will be shared with the ERC in the Privacy Notices for the Department's pupil databases. For the ERC to collect the personal data concerned would take considerable time, be liable to error and duplication of existing data capture for the same reason. The transfer of pupil personal data and school attributes allows the ERC to administer the tests in an efficient manner to all schools together; speeding the process; ensuring a secure transfer of personal data and; without duplication of schools supplying the same data twice to both the Department and an agency acting on behalf of the Department. The ERC shares that data with the participating school in order to validate the accuracy of the data. This same data was originally supplied to the Department by the participating school itself. The legal basis for the ERC to share that data with the participating school is SI 392 of 2015 (Educational Research Centre (Establishment) Order 2015) sections 7, 8 and 9. The functions of the ERC under the SI are to maintain systems for the benefit of schools that will enable them to assess the attainment levels and academic standards of students as required under the Education Act, to assist schools in fulfilling their obligations under the Education Act, to maintain and publish information on the attainment levels and academic standards of students in schools and to conduct independent research on all aspects of education. The Educational Research Centre carries out various studies at a national and international level on behalf of the Department of Education. A major purpose of studies such as **PIRLS (Progress in International Reading Literacy Study), TIMSS (Trends in International Mathematics and Science Study) & PISA (The Programme for International Student Assessment)** is to provide background information that can be used to improve teaching and learning. For example, the study collects detailed information about curriculum and curriculum implementation, instructional practices, and school resources. The assessment is based on comprehensive frameworks developed collaboratively with the participating countries. The frameworks specify in some detail the knowledge, skills, and understandings to be assessed. **For PIRLS and TIMSS**, the data will be used to assign passwords to selected pupils so that they can complete electronic tests of reading literacy (PIRLS), mathematics and science (TIMSS), and electronic questionnaires (field trial), and to assign instruments so that they can complete paper-based or digital tests and questionnaires (main study). Pupil names will also be

	used to communicate with parents regarding their children's participation, and to request them to complete a parent questionnaire. **For PISA** a fixed number of 15-year-olds in each school will be selected at random and will be invited to complete the online PISA tests in reading literacy, mathematics and science, and an online questionnaire. Pupil names will also be used to contact the parents of participating pupils regarding their child's participation in PISA, and to request them to complete a parent questionnaire. **NAMER (National Assessments of Maths & English Reading)** provides important information for policymakers on primary schools in Ireland. The assessments provide information on Reading and Mathematics achievement in primary school children as a group. The questionnaires issued in parallel provide context for this data. NAMER is also used to understand Maths and Reading skill. This type of knowledge can be used to inform curriculum development and future test development as well as classroom teaching. Pupil names are not used on test booklets and questionnaires. Pupil names appear only on a 'Class list that is sent by registered post to the nominated school coordinator. Tests are administered by class teachers; testing is supervised by the nominated school coordinator. A Department of Education inspector oversees testing in 20% of schools. **DEIS – (Delivering Equality of opportunity In Schools)** Work by the ERC, on behalf of the Department of Education, began in 2007 on an ongoing independent evaluation of the SSP (School Support Programme) component of DEIS in primary and post-primary schools. Since then, the evaluation has been monitoring implementation of the programme and assessing its impact on participants. Periodic monitoring of achievement and other pupil outcomes has been a key feature of the evaluation at primary level since 2006/07. **GSRS (Gaeltacht Schools Recognition Scheme)** - The Gaeltacht School Recognition Scheme (Scheme) was launched by An tAonad um Oideachas Gaeltachta in the Department of Education in April 2017 as part of the overall implementation of the Policy on Gaeltacht Education 2017-2022. The objective of the Scheme is to support the use of the Irish language in Gaeltacht communities by enhancing and promoting the delivery of high-quality Irish-medium education in Gaeltacht schools. The Scheme has been extended to the end of 2024. The objective of the Research and Evaluation Study is to evaluate the impact of the Scheme on the provision of education through the medium of Irish in primary and post-primary schools participating in the Scheme and the extent to which they are fulfilling the language-based criteria to strengthen immersion education. Names of pupils will be used to label test booklets and questionnaires, to ensure a match between booklets and pupil questionnaires, to contact parents

	about their child's participation in the study, and to request them to complete a parent questionnaire. When schools are sampled to participate in these studies, the ERC provides the Department of Education with the list of schools and the classes sampled for that given study, along with the data required for each student and school. The data requested for PIRLS, PISA, TIMSS and NAMER relate to names of pupils, their dates of birth, their gender, and, where relevant, their school programme and grade level. The data are used to facilitate the administration of assessments in schools and to ensure representativeness when selecting samples. Access to pupil information from the DE POD and P-POD systems means that the ERC does not have to request this information directly from schools making the process more efficient. This, in turn, facilitates more timely administration of studies, and increases data security. Personal data held by the ERC are retained only as long as required to fulfil the function for which the personal data is required.

Table 2.3

3. Data to be shared

3.1 Quality

The Parties will take all reasonable steps to ensure that any personal data processed under this agreement is accurate, kept up to date, and that data which is inaccurate, having regard to the purposes for which it was processed, is erased or rectified as soon as is practicable.
Shared personal data shall be limited to the personal data described in table 3.4 to this agreement and will be shared only in the manner as set out in table 11.2 therein. Where a party receiving data is notified of inaccurate data by the data subject, this party is obliged to notify the disclosing Party/Lead Agency.

3.2 Subject Rights

In so far as the shared personal data is processed by the Party/Parties receiving data, as a data controller, the Party/Parties receiving data will deal with data subjects in their exercising of rights set out in the GDPR, including but not limited to, the right of access, the right of rectification, erasure, restriction of processing and to data portability.

Data subjects have the right to obtain certain information about the processing of their personal data through a data subject access request.

Data subject access requests in relation to data processed by the Party/Parties receiving data will be dealt with by them directly. Data subject access requests in relation to data processed by the Party/Parties disclosing data prior to the transfer will be dealt with by them directly.

3.3 Sharing with Third Parties

The Party/Parties receiving data shall not share the shared personal data with any person who has not been authorised to process such data.

3.4 Detail of the information to be disclosed

Provide details of the personal data set to be disclosed and the detail of any non-personal data.

Note:

If the non-personal data and personal data are linked together to the extent that the non-personal data becomes capable of identifying a data subject then the data protection rights and obligations arising under the GDPR will apply fully to the whole mixed dataset, even if the personal data represents a small part of the set.

	DESCRIPTION
Shared Personal Data	• Pupil's/Student's name • date of birth • gender • class name (label used by school e.g. at primary level Ms. Murphy's class / at post-primary level 2A, 2 Oak,) • programme level (i.e. Junior Cycle, Transition Year, Leaving Cert) • grade level – e.g. Fourth Class, Second Year Parental data is not shared by the Department with the ERC.

Non-personal Data	• School roll number. • HP Deprivation index for schools - (numbers and percentages in various HP 'bins', mean school HP score, school standard deviation on HP score). • Percentage of students in a school from particular ethnic groups (e.g., Traveller and/or Roma) and the percentage of students categorised as EAL (English as an Additional Language). • Aggregated data (STen score distributions, gender, numbers of exemptions) for English reading, Irish reading and mathematics in respect of primary schools in the Gaeltacht Schools Recognition Scheme and for DEIS.

Table 3.4

4. Function of the Parties

4.1 Function of the Parties

In table 4.1 below:

i. Specify the function of the party disclosing data to which the purpose (as defined in table 2.3) of the data sharing relates

ii. Specify the function of the party receiving data to which the purpose (as defined in table 2.3) of the data sharing relates.

	PARTY	FUNCTION
i.	**Department of Education disclosing data**	It is a function of the Minister for Education under section 7 of the Education Act 1998 as amended to ensure that there is made available to each person resident in the State a level and quality of education appropriate to meeting the needs and abilities of that person, to determine national education policy, and to plan and co-ordinate the provision of education in recognised schools. It is also a function of the Minister under the Act to monitor and assess the quality, economy, efficiency and effectiveness of the education system provided in the State by recognised schools and to publish, in such manner as the Minister considers appropriate, information relating to such monitoring and assessment. Section 7 of the Act states: *"(1) Each of the following shall be a function of the Minister under this Act:* *(a) to ensure, subject to the provisions of this Act, that there is made available to each person resident in the State, including a person with a disability or who has other special educational needs, support services and a level and quality of education appropriate to meeting the needs and abilities of that person,* *(b) to determine national education policy, and* *(c) to plan and co-ordinate—* *(i) the provision of education in recognised schools and centres for education, and* *(2) Without prejudice to the generality of subsection (1), each of the following shall be a function of the Minister:* *(b) to monitor and assess the quality, economy, efficiency and effectiveness of the education system provided in the State by recognised schools and centres for education, having regard to the objects provided for in section 6 and to publish, in such manner as the Minister considers appropriate, information relating to such monitoring and assessment;"*

ii.	**Educational Research Centre receiving data**	In September 2015, the Educational Research Centre was designated as a Statutory Body in accordance with the Education Act1998 as amended - see S.I. No. 392/2015 Educational Research Centre (Establishment) Order 2015 and S.I. No. 309/2017 Educational Research Centre (Establishment) (Amendment) Order 2017. The functions of the Centre are to: (a) provide an assessment support service to schools and centres for education that will enable them to fulfil their obligations under Section 9 of the Education Act; and (b) conduct independent research on all aspects of education and at all levels of the education system including educational research that will inform policy making and the improvement of educational standards. The ERC administers international and national studies on behalf of the Department of Education, including PISA, PIRLS and NAMER. In addition, the ERC implements programme evaluations (e.g., Gaeltacht Schools Recognition Scheme). SI 392 of 2015 states: *"7. The Centre, acting within the policy set by the Minister for Education and Skills in accordance with Section 54 (2) of the Education Act 1998 , shall:* *(a) provide an assessment support service to schools and centres for education that will enable them to fulfil their obligations under Section 9 of the Education Act, 1998 ;* *(b) conduct independent research on all aspects of education and at all levels of the education system including educational research that will inform policy making and the improvement of educational standards.* *8. To further the objects in Article 7 above, the functions of the Centre shall be to develop and provide materials to schools, and establish and maintain systems for the benefit of schools, that will:* *(i) enable them to assess the attainment levels and academic standards of students as required under Section 9 (k) of the Education Act, 1998 ;* *(ii) enable them to report systematically on the attainment levels and academic standards of students to parents, students, boards of management, the Minister for Education and Skills and others;* *9. To enable the functions of the Centre as set out in Article 8 above, the activities of the Centre shall include, but not necessarily be limited to:* *(b) carrying out national and international assessments of the attainment levels and academic achievement of students and reporting on such assessments to the Minister;*

	(c) maintaining, storing securely and publishing information on the attainment levels and academic standards of students in schools and centres for education in Ireland; *(k) doing all such acts and things as may be necessary to further the objects of the Centre."*

Table 4.1

5. Legal Basis

5.1 Legal Grounds

For the purposes identified in this Data Sharing Agreement the Parties confirm that the sharing and further processing of the defined personal data is based on the legal grounds set out in 5.1.1 and 5.1.2.

5.1.1 Appropriate Legislative Provisions for Sharing

Define the appropriate legal provision for sharing based on the following:

i. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art 6. 1 (e)

Specify the legal obligation for sharing in the table below.

LEGISLATION	DESCRIPTION
I[s.13 2 a) ii) V, VI, VII and VIII	A public body may disclose personal data to another public body in a case in which this section applies to such disclosure, only where – (a) the personal data concerned is disclosed (i) for the purpose of the performance of a function of the first or second mentioned public body, and (ii) for one or more of the following purposes (V) to facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body; (VI) to facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body; (VII) to enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body; (VIII) to facilitate an analysis of the structure, functions, resources and service delivery methods of the first or second mentioned public body.

Table 5.1.1

5.1.2 Appropriate Legislative Provisions for Further Processing

Specify the appropriate legal provision for further processing based on the following:

i. processing is necessary for compliance with a legal obligation to which the controller is subject; (GDPR Art 6. 1 (c))

LEGISLATION	DESCRIPTION
(GDPR Art 6. 1 (c))	Section 7 of the Education Act 1998 as amended S.I. 392/2015 Educational Research Centre Establishment Order 2015, with specific reference to Articles 7, 8 and 9 '7. The Centre, acting within the policy set by the Minister for Education and Skills in accordance with *Section 54* (2) of the *Education Act 1998* , shall: b) conduct independent research on all aspects of education and at all levels of the education system including educational research that will inform policy making and the improvement of educational standards. 8. To further the objects in Article 7 above, the functions of the Centre shall be to develop and provide materials to schools, and establish and maintain systems for the benefit of schools, that will: II. enable them to report systematically on the attainment levels and academic standards of students to parents, students, boards of management, the Minister for Education and Skills and others; 9. To enable the functions of the Centre as set out in Article 8 above, the activities of the Centre shall include, but not necessarily be limited to: a) providing advice to schools and centres for education on the assessment of the attainment levels and academic standards of students; b) carrying out national and international assessments of the attainment levels and academic achievement of students and reporting on such assessments to the Minister; c) maintaining, storing securely and publishing information on the attainment levels and academic standards of students in schools and centres for education in Ireland; d) engaging in the evaluation of educational programmes and activities; e) initiating and conducting research consistent with the objects of the Centre, and publishing and disseminating the findings of this research; h) co-operating with other bodies, as appropriate, in research, assessment and evaluation studies and in the dissemination of findings concerning research, assessment and evaluation; j) co-operating with other bodies, as appropriate; k) doing all such acts and things as may be necessary to further the objects of the Centre.'

Table 5.1.2

6. Impetus for Data Sharing

Specify the impetus (the motivation or where benefits will be realised) in relation to the data shared under this agreement.

THE IMPETUS FOR THE DISCLOSURE OF DATA WILL COME FROM:	TICK AS APPROPRIATE
i. Data subject	☐
ii. Public Body	☒

Table 6.0

7. Categories of Data Shared

The personal data shared may be in relation to individual data subjects and/or classes of data subjects. Classes of data subject may be defined by the parties involved and some examples might be customers, vendors, suppliers, visitors, etc.

Aggregated data is information gathered and expressed in a summary form for purposes such as statistical analysis, and so is not personal data for the purposes of data protection law and GDPR and is not the same as classes of data subject.

Select from the below table and comment as appropriate.

CATEGORY		COMMENT
Individual Data Subject	☒	Pupils/Students
Classes of Data Subjects	☒	Data for primary school pupils are required for PIRLS, TIMSS Grade 4, NAMER, DEIS and GSRS studies. Data for secondary school students are required for PISA, TIMSS Grade 8, DEIS and GSRS studies

Table 7.0

8. Duration and Frequency

8.1 Duration

Define the start and end dates of the information transfer:

The Data Sharing Agreement will commence on the 1st of December 2023 and continue until the parties agree to terminate agreement*/*

8.2 Frequency

Indicate the type of transfer that will be required with a description.

TYPE		DESCRIPTION
Once off	☐	
Frequent/regular updates	☒	Monitoring and evaluation of the DEIS programme is ongoing and data may be requested for specific strands of work as needed as agreed with the Social Inclusion Unit of DE
Other frequency	☒	TIMSS, PIRLS, PISA, and NAMER operate on specific cycle at 3, 4, 5 or 6-year intervals. Data is only requested for each study for the Field Trial (occurring the year prior to the Main Study) and the Main Study for the relevant cycle of the specific study. The Gaeltacht School Recognition Scheme study is due to be completed in 2024 and requires the data outlined in this Data Sharing Agreement to complete the project. Data sent based on requirements usually following the academic cycle

Table 8.2

9. How data will be processed

9.1 Obligations of the Parties in Respect of Fair and Lawful Processing

Each Party shall ensure that it processes the shared personal data fairly and lawfully. Each will comply with the requirements of the Data Protection Act 2018, GDPR and any legislation amending or extending same, in relation to the data exchanged.

Each Party undertakes to comply with the principles relating to the processing of personal data as set out in Article 5 GDPR, in the disclosing of information under this Data Sharing Agreement.

Both Parties shall, in respect of shared personal data, ensure that they provide sufficient information to data subjects in order for them to understand what components of their personal data the Parties are sharing, the purposes for the data sharing and either the identity of the body with whom the data is shared or a description of the type of organisation that will receive the personal data.

9.2 Description of Processing

Include a description of how the disclosed information will be processed by each receiving party.

	DESCRIPTION OF PROCESSING
Education Research Centre	The data shared by the DE about the sampled schools, is subsequently shared by the ERC with the relevant school. This data was originally provided to DE by the sampled school itself. Each sampled school is asked to review the data for their schools, provided by the DE in order to validate the accuracy of the data. Where a student from the sampled set is no longer in that class/school, or where a new student in the class is not represented in the data shared by the DE with the ERC, the school is asked to correct the data, adding new students and removing any students where relevant. **For PIRLS and TIMSS**, the data will be used to assign passwords to selected pupils so that they can complete electronic tests of reading literacy and electronic questionnaires (field trial), and to assign instruments so that they can complete individually assigned paper-based tests and questionnaires (main study). Pupil names will also be used to communicate with parents regarding their children's participation, and to request them to complete a parent questionnaire. The personal data referred to above will be requested in the autumn prior to testing. **For PISA** a fixed number of 15-year-olds in each school (defined as those born in a specific calendar year) will be selected at random and will be invited to complete the online PISA tests in reading literacy, mathematics and science, and an online questionnaire. Pupil names will also be used to contact the parents of participating pupils regarding their child's participation in PISA, and to request them to complete a parent questionnaire. The personal data referred to above will be requested in the spring prior to testing.

	For NAMER Pupil names will not be used on test booklets and questionnaires. Pupil names appear only on a 'Class list' that is sent by registered post to the nominated school coordinator. Tests are administered by class teachers; testing is supervised by the nominated school coordinator. A Department of Education inspector will oversee testing in approximately 20% of schools. Schools distribute an information letter about the study to parents at least four days before the administration of the study. These data will be requested in the autumn or winter prior to testing. **For GSRS** Names of pupils will be used to label test booklets and questionnaires, to ensure a match between booklets and pupil questionnaires, to contact parents about their child's participation in the study, and to request them to complete a parent questionnaire. For additional information, please refer to sections 9.3 (Further Processing), 10 (Restrictions), 11 (Security Measures), 12 (Retention) and 13 (Methods Used to Destroy/Delete Data)

Table 9.2

9.3 Further Processing

i. Specify any further processing by the Party or Parties receiving data of the personal data disclosed by the disclosing body under this Data Sharing Agreement.

	SPECIFY FURTHER PROCESSING

Table 9.3.1

10. Restrictions

Specify any restrictions on the disclosure of information after the processing by the Party or Parties receiving data to the personal data disclosed by the disclosing body under this Data Sharing Agreement. Give a description of the restrictions, if any, which apply to the further disclosure of the information in table 10.0 below.

	RESTRICTIONS ON DISCLOSURE AFTER PROCESSING
Educational Research centre	For the purposes of the data requested under this agreement, the ERC combines the data provided by the Department of Education with data collected from the data subject (e.g., pupil test results, questionnaire data). Pseudonymised data is shared with contractors working with the IEA (PIRLS and TIMSS) and the OECD (PISA), and with our data entry provider. In these scenarios, where personal data is shared outside of the ERC to achieve the project outcomes, the ERC has a GDPR compliant Data Processor Agreement in place to safeguard the data shared, with public interest derogation used in the case of PISA. Personal identifiers (student names and dates of birth) are removed/replaced in accordance with the guidelines of the OECD and IEA. Two years after the completion of the Main Study, all personal data gathered to deliver the study are anonymised. No data is released at school level (roll number) which can be used to create a league table.

Table 10.0

11. Security Measures

11.1 Security and Training

Both Parties shall adhere to the procedures set out in table 11.2 below, regarding the transfer and receipt of data.

The Party/Parties receiving data agree, in accordance Article 32 of the GDPR, to implement appropriate technical and organisational measures to protect the shared personal data in their possession against unauthorised or unlawful processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the shared personal data transmitted, stored or otherwise processed.

This may include, but is not limited to:

- Policies, guidelines and procedures governing information security.
- Password protection for computer access.
- Automatic locking of idle PCs.
- Appropriate antivirus software and firewalls used to protect integrity and security of electronically processed data.
- Unique identifiers for every user with access to data.
- Employees have access only to personal data required for them to do their jobs.
- Appropriate security where remote access is allowed.
- Encryption of data held on portable devices.
- Data breach procedures.
- Appropriate physical security.
- Staff training and awareness.
- Monitoring of staff accessing data.
- Controlling physical access to IT systems and areas where paper-based data are stored.
- Adopting a clear desk policy.
- Appropriate techniques for destruction of data.
- Having back-ups of data off-site.

Both Parties shall ensure that the security standards appropriate to the transfer of personal data under this agreement are adhered to.

The Party/Parties receiving data shall ensure that all persons who have access to and who process the personal data are obliged to keep the personal data confidential.

The Party/Parties receiving data shall ensure that employees having access to the data are properly trained and aware of their data protection responsibilities in respect of that data.

Access to the data supplied by the Party disclosing data will be restricted to persons on the basis of least privilege, sufficient to allow such persons carry out their role.

Each Party will keep the data secure and ensure that it is transferred securely in accordance with the procedures of this agreement.

11.2 Security Measures

For the purpose of this agreement, particular regard should be given to the data safeguards outlined in the following sections and subsections:

- 11.2.1 – Lead Agency/Party Disclosing Data
- 11.2.2 – Party/Parties Receiving Data
- 11.2.3 – Data Breaches and Reporting

11.2.1 Lead Agency/ Party Disclosing Data

The following questions should be completed by the Lead Agency/ party disclosing data in the data sharing arrangement.

All questions should be answered in a manner that does not compromise any security measures in place.

11.2.1.1	TRANSMISSION	COMPLIES	DOES NOT COMPLY
	When data is being transmitted from the Lead Agency/party disclosing data to the party/parties receiving data, robust encryption services (or similar) are in use. Please provide details.	☒	☐
		Data is transferred using the Secure File Transfer Protocol which includes Secure Shell protocol encryption.	

Table 11.2.1

11.2.1.2 – SECURITY STATEMENT
Give an outline of the security measures to be deployed for transmission of personal data, in a manner that does not compromise those security measures. You may also provide details of additional measures in place for the sharing of data that are relevant to this arrangement.
The Department implements multiple cybersecurity protocols and measures including 24x7 IT Security Monitoring, User Awareness, Perimeter Security, Anti-virus/Anti-Malware, Email and Web filtering, System Patching, Risk Management, Policies, Regular Vulnerability Assessments/Penetration Testing, Mobile Device Management, Access Management, Incident Management, Event Monitoring, Information Security Governance, GDPR Awareness, Disaster Recovery, Offline backups, Supplier Management and Encryption. As a matter of policy we do not disclose details of systems and processes which could in any way compromise the Department's information security posture.

11.2.1.3 SECURITY SPECIALIST FOR LEAD AGENCY	YES/NO
Please confirm your security specialist has reviewed this Data Sharing Agreement and that their advice has been taken into consideration.	YES

Table 11.2.2

11.2.2 Party/Parties Receiving Data

The following questions should be completed by the Party receiving the disclosure of data as part of this Data Sharing Agreement.

Where a 'not applicable' response is included, ensure information is provided as to why.

All questions should be answered in a manner that does not compromise any security measures in place.

11.2.2	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.1	**In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐
11.2.2.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒	☐	☐
		Staff only have access to data that is required to carry out their work. This is the same for remote working where staff access data over a VPN and still only have access to the same data as when working on site.		
11.2.2.3	**A least privileged principle (or similar) is in place to ensure that users are authenticated proportionate with the level of risk associated to the access of the data.** Please provide details.	☒	☐	☐
		Complies, staff only have access to data they require. Data is secured on ERC servers that is based in an IT Secure room with access controls enabled. Staff only have access to data that they require to carry out the functions of their role. All other drives and folders are not visible. All staff have their own AD network logon and VPN username and password to be used if working remotely. Updated IT Policies have been rolled out this year to inform staff about new security measures. 2FA is enabled for all staff for Office365 cloud storage.		

11.2.2.4	**Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).** Please provide details of the protections in place and how they are managed.	☒	☐	☐
		The access of unauthorised persons to the ERC building and to the data processing systems is denied using the following measures. **Entrance control:** - Building access control system - Building alarm system - Secured IT server room - Employee references checked prior to employment - Specified cleaning and maintenance times - Guests and external service providers are accompanied. **Access controls:** The unauthorised use of the data processing systems is prevented by the following measures: - Use of encryption on servers - Specified user account for each employee - Authentication of user access with password via Active Directory - Automated screen lock - Dedicated network folders for projects and associated data - Employee hiring and leaving processes. - Restricted Network Folder Access All hard and soft copy data will be stored securely at the ERC or in secure storage.		
11.2.2.5	**Data is encrypted at rest on mobile devices such as laptops and removable media.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐

11.2.2.6	There are policies, training and controls in place to minimise the risk that data is saved outside the system in an inappropriate manner or to an inappropriate, less secure location. Please provide details.	☒	☐	☐
		Staff training on information protection and privacy matters – upon commencement of employment with the ERC, employees receive data protection training. Project Managers have also been trained on the completion of the Data Protection Impact Assessment tool and all new projects are reviewed and risk assessed for any potential concerns for personal data pertaining to their security and protection. All employees receive refresher training and project team members participate in the DPIA process to ensure they are aware of the potential risks to data for the projects they work on. Employees are required to immediately report security incidents to the Data Protection Officer, who will take care of further coordination and handling of the incident. When working with data, whether working with digital data using IT systems and applications or working with data in hard copy formats, the ERC's employees must comply with the applicable data protection legislation as well as the ERC's policies and procedures. If employees are unsure about the application of the procedures, policies or as to whether and to what extent legislation must be observed, they should contact their manager or the Data Protection Officer for clarification. **Confidentiality clauses in employee contracts** – all employees of the ERC have a confidentiality clause included in their employment contract and have a contractual obligation to ensure the security and integrity of the data they work with. Failing to comply with these requirements may lead to disciplinary proceedings. The importance of ensuring confidentiality is emphasised to all staff and reflected in staff contracts, including short-term staff. All sensitive files will also be password-protected or restricted to relevant staff. All ERC and external providers signed confidentiality agreements and are made		

		aware (through contracts and training (where appropriate)) of their obligations to report a breach, disclosure or loss of personal information
11.2.2.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	**Back up and archiving measures** – Files, folders and servers are backed up on a regular basis. Tapes are securely stored offsite. **Malware protection** – Antivirus-Software is installed. Procedures in place to deal with any infection of IT systems. Security updates and patches are promptly installed. **Data recovery procedures** – The ERC has its own internal backup procedure. The ERC will track the upload status of pupil and student data and the number of uploads will be cross-referenced against the Technical Support (TS) Form (completed by Technical Support and received on the day of the assessment). Each study has a check-back process .
11.2.2.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	Data will be anonymised after the processing of data is complete (for example, checking the quality of data). Generally, this may take up to 24 months after the tests are administered. Data stored on devices such as USBs are pseudonymised back-up data and will be deleted once the ERC team has carried out necessary data checks and where the data is verified. The practice of using USB keys is applied in limited circumstances where there is no suitable, alternative arrangement. USB keys are not used to store or transfer the data shared under this agreement. Data will be stored on secure ERC servers with physical access controls enabled

Table 11.2.3

11.2.2.9 – SECURITY STATEMENT
Give an outline of the security measures to be deployed for the storage and accessing of personal data, in a manner that does not compromise those security measures. You may also provide details of additional measures in place that are relevant to this arrangement.
Data is secured on ERC servers with physical access controls enabled. Staff only have access to data that they require to carry out the functions of their role. All staff have their own AD network logon and VPN username and password to be used if working remotely. Updated IT Policies have been rolled out this year to inform staff about new security measures. The ERC does not disclose details of systems and processes which could in any way compromise its information security posture. For additional information, please refer to sections 9.2 (Description of Processing) 9.3 (Further Processing), 10 (Restrictions), 12 (Retention) and 13 (Methods Used to Destroy/Delete Data)

11.2.2.10 SECURITY SPECIALIST FOR PARTY/PARTIES RECEIVING DATA	YES/NO
Please confirm the security specialist(s) Party/Parties receiving have reviewed this Data Sharing Agreement and that their advice has been taken into consideration.	YES

Table 11.2.4

11.3 Data Breaches and Reporting

If a personal data breach occurs after the data is transmitted to the Party/Parties receiving data, the Party/Parties receiving data will act in accordance with the Data Protection Commission's Breach Notification Process and in accordance with GDPR requirements.

12. Retention

Define the retention requirements for the disclosed information for the duration of the Data Sharing Agreement and in the event the agreement is terminated, for:

1. the information to be disclosed and
2. the information resulting from the processing of that disclosed information

INFORMATION TYPE	RETENTION REQUIREMENTS
1. **Information to be disclosed**	The information will be **destroyed** after the period of two years when a cycle of testing can been completed
2. **Information resulting from the processing of the data**	Retained in anonymised format. For additional information, please refer to sections 9.2 (Description of Processing) 9.3 (Further Processing), 10 (Restrictions), 11 (Security Measures) and 13 (Methods Used to Destroy/Delete Data

Table 12.0

13. Methods Used to Destroy/Delete Data

Detail how information will be destroyed or deleted at the end of the retention period as defined in the Data Sharing Agreement, for:

1. the information to be disclosed and
2. the information resulting from the processing of that disclosed information

INFORMATION TYPE	DESCRIPTION
1. Information to be disclosed	The data will be anonymised or deleted in line with internal ERC guidelines. ERC project staff working with the data transferred by the DoE, delete personal identifiers (e.g., names) from databases to anonymise datasets. They review all documents with student identifiers to delete or anonymise those identifiers, in order to ensure an individual student cannot be identified from the data that is retained. Hard copy documentation is confidentially shredded using the services of an on-site shredding company.
2. Information resulting from processing of the data	Not applicable – the anonymised information is retained for the purposes of reporting to the Department or Education

Table 13.0

14. Withdrawal from Agreement

14.1 Procedure

Each Party commits to giving a minimum of 90 days notice of its intention to withdraw from or terminate this Data Sharing Agreement.

Each Party disclosing personal data pursuant to this Agreement reserves the right to withdraw, without notice, access to such data where that Party has reason to believe the conditions of this Data Sharing Agreement are not being observed. Each Party disclosing data will accept no responsibility for any consequences arising from the exercise of this right.

Where the disclosing Party is subsequently satisfied that the conditions of the Data Sharing Agreement are being observed, access will be restored forthwith.

Where access to shared personal data is withdrawn, the withdrawing Party shall provide to the other Party reasons for that withdrawal as soon as is practicable thereafter. Where there are only 2 Parties, withdrawal by either one shall be considered a termination of the agreement. Where an agreement has multiple Parties and one withdraws, the Lead Agency should update the schedule and inform the other Parties to the agreement.

Where a Data Sharing Agreement expires or is terminated, the Lead Agency shall notify the Minister in writing within 10 days of the withdrawal. The Lead Agency shall also notify the Data Governance Board as soon as practicable after such expiration or termination, as the case may be.

14.2 Severance

If any provision of this agreement (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of this agreement, and the validity and enforceability of the other provisions of this agreement shall not be affected.

15. Other Matters

15.1 Variation

No variation of this agreement shall be effective unless it is contained in a valid draft amendment agreement executed by the Parties to this Data Sharing Agreement in accordance with the procedures and requirements set out in Part 9, chapter 2 of the Data Sharing and Governance Act 2019.

15.2 Review of Operation of the Data Sharing Agreement

The Parties shall review the operation of the Data Sharing Agreement on a regular basis, with each such review being carried out on a date that is not more than 5 years from:

i. in the case of the first such review, the date on which the Data Sharing Agreement came into effect, and
ii. in the case of each subsequent review, the date of the previous review. A review under s.20(1) shall consider the impact of the technical, policy and legislative changes that have occurred since the date of the previous review under s.20(1).

Where the Parties to the Data Sharing Agreement consider that it is appropriate following completion of a review they shall prepare an amended Data Sharing Agreement to take account of the technical, policy and legislative changes that have occurred since the date of the previous review or the effective date. The amended agreement will be executed by the Parties in accordance with the procedures and requirements set out in Part 9, chapter 2 of the Data Sharing and Governance Act 2019.

15.3 Jurisdiction

This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of the Republic of Ireland.

15.4 Indemnity

The Party/Parties receiving data shall indemnify and keep indemnified the Party/Parties disclosing data, in full, from and against all claims, proceedings, actions, damages, losses, penalties, fines, levies, costs and expenses, whether direct or indirect and all consequential or indirect loss howsoever arising out of, in respect of or in connection with any breach by the Party/Parties receiving data, including their servants, of data protection requirements.

15.5 Publication

15.5.1 Public Consultation and publishing a Notice

Public Consultation is managed on behalf of the parties by the Data Governance Unit in OGCIO. Each of the proposed parties will be required to publish, on the same date as the consultation, a notice on their website that they are proposing to enter into the DSA. They should state the documents that are accessible to the public and link to their relevant DSA and DPO statements published on the public consultations website. This notice should invite submissions and include the date of publication of the notice.

15.5.2 Publishing Executed DSA

After each of the Data Governance Board recommendations have been addressed by the parties and after this Data Sharing Agreement has been signed by appropriate Authorised Signatories, the Lead Agency in respect of this Data Sharing Agreement shall publish a copy of the final agreement on a website maintained by it as soon as practicable after sending a copy of the agreement to the Data Governance Unit who will accept it on behalf of the Minister.

15.6 Base Registries

In respect of this Data Sharing Agreement, where the personal data disclosed is contained in a Base Registry, the Base Registry owner will take on the role of Lead agency.

16. Schedule A - Data Protection Impact Assessment

If a data protection impact assessment (DPIA) has been conducted in respect of the data sharing to which this Data Sharing Agreement relates, a summary of the matters referred to in Article 35(7) of the GDPR is required to be filled in the table below.

OR

If a data protection impact assessment has not been conducted as it is not mandatory where processing is not "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35 of the GDPR), outline the reasons for that decision in the table below.

DPIA	Select	SUMMARY OF DATA PROTECTION IMPACT ASSESSMENT
Has been conducted	☒	The DPIA between the ERC and DoE assess the risks, highlights the potential impact, and outlines the measure to ensure data protection. Any risks identified have been satisfactorily mitigated against. The data will be collected by the DoE which is used for grants and teacher allocation stored on secure database with limited password access. The personal data of students will be transferred to the ERC upon request to conduct research on behalf of the DoE. These studies include PIRLS, TIMSS, PISA, NAMER, DEIS and GSRS. The data is processed by DoE under the Education Act (1998) and by the ERC under S.I. No. 392/2015 Educational Research Centre (Establishment) Order 2015 and S.I. No. 309/2017. The risks involved relate to Large-Scale Processing: Data to be processed are at a large scale. Profiling: Evaluating and scoring of pupils and school types. Tracking: Pupils moving through the schooling system. Data Matching: Processing of school with DEIS status data sets for statistical analyses. Processing data relating to children: Processing personal data related to the children in primary and post-primary schools.

		These risks will not affect the rights of the data subjects to be informed, access, rectification, erasure, restrict processing, portability and the right to object, profiling and automated decision-making. The data is secured on restricted drives with accessibility limited to approval personal using secure credentials in both organisations. Data will be transferred from DoE to ERC using Secure File Transfer Protocol using encryption and password protection.
Has not been conducted	☐	

Table 16.0

Note: If the Data Sharing Agreement is amended to reflect a change in the scope, form or content of the data processing, then there is an obligation on the data controllers to consider whether the changes give rise to a high risk to the rights and freedoms of natural persons, such that a DPIA should be carried out.
Under S.20(4) of Data Sharing and Governance Act, an amended draft agreement must be submitted for review to the Data Governance Board in accordance with Part 9, Chapter 2 of the Data Sharing and Governance Act.

17. Schedule B

17.1 Necessary for the Performance of a Function

Outline the reasons why the disclosure of information under this agreement is necessary for the performance of the relevant function and explain why it is proportionate in that context.

It is a statutory function of the Minister for Education under the Education Act 1998 as amended to ensure that there is made available to each person resident in the State a level and quality of education appropriate to meeting the needs and abilities of that person, to determine national education policy, and to plan and co-ordinate the provision of education in recognised schools. It is also a function of the Minister under the Act to monitor and assess the quality, economy, efficiency and effectiveness of the education system provided in the State by recognised schools and to publish, in such manner as the Minister considers appropriate, information relating to such monitoring and assessment.

It is a function of the Educational Research Centre under S.I. 392 of 2015 to provide an assessment support service to schools and to conduct independent research on all aspects of education and at all levels of the education system including educational research that will inform policy making and the improvement of educational standards. The ERC carries out various studies on a national and international level on behalf of the Minister for Educations in order to

- Provide an assessment support service to schools and centres for education that will enable them to fulfil their obligations under Section 9 of the Education Act 1998
- Conduct independent research on all aspects of education and at all levels of the education system including educational research that will inform policy making and the improvement of educational standards.

For the ERC to collect the personal data concerned would take considerable time, be liable to error and duplication of existing data capture for the same reason. The transfer of pupil personal data and school attributes allows the ERC to administer the tests in an efficient manner to all schools together speeding the process, ensuring a secure transfer of personal data and without duplication of schools supplying the same data twice to both the Department and an agency acting on behalf of the Department.

17.2 Safeguards

Summarise the extent to which the safeguards applicable to the data shared under this agreement are proportionate, having regard to the performance of functions by the Parties and the effects of the disclosure on the rights of the data subjects concerned.

The personal data concerned is relatively limited and does not contain any special category data.

Testing of pupils requires the identification of pupils within a classroom. The personal data provided (name, date of birth, gender, and teacher's name) would have been collected by the ERC to conduct these tests in the past. The provision of this data allows the ERC to administer the tests in an efficient manner. No additional data is provided beyond what the ERC would have previously collected to allow the correct identification a pupil

The Department and the ERC have a range of safeguards in place, both from an IT perspective and a data protection perspective. Both organisations have strong IT security, data back-ups and access controls in place. Both organisations have a range of data protection policies and procedures in place and staff are trained in compliance. See section 11 for additional information outlining these measures in detail.

It is considered that the safeguards are proportionate given the functions of the parties involved and the fact that the data sharing is ultimately of benefit to the data subject in terms of improving the quality of education.

18. Schedule C

18.1 List of Parties to this Agreement

Set out the names of all the Parties to the agreement.

As required under S.21 (3)(a), (b) and (c) of the Data Sharing and Governance Act 2019, this Schedule must be updated by the Lead Agency to include any Parties who have joined the agreement by way of an Accession Agreement, and to remove any Party that has withdrawn from the agreement. The Lead Agency must notify the other Parties of any amendments to this Schedule and the Data Governance Board.

[**Lead PSB -** The Department of Education
Other PSB - The Educational Research Centre

19. Authorised Signatory

An authorised signatory is required to sign this Data Sharing Agreement after all recommendations made by the Data Governance Board have been addressed and before the Data Sharing Agreement can be executed.

This signatory has the role of accountability for the data sharing defined in this Data Sharing Agreement and holds the post of Principal Officer (equivalent) or above.

The Parties hereby agree to their obligations pursuant to this Data Sharing Agreement for the transfer of personal data as described in this Data Sharing Agreement.

19.1 Lead Agency

LEAD AGENCY			
Signature:	Paul John Alexander	**Date:**	Nov 24, 2023
Print Name:	Paul Alexander		
Position held:	[Senior Statistician Principal Officer]		
Email:	Paul_Alexander@education.gov.ie		
For and on behalf of:	[The Department of Education]		

Table 19 .1

19.2 Other Party/Parties

OTHER PARTY			
Signature:	John Regan	**Date:**	Nov 23, 2023
Print Name:	John Regan		
Position held;	[CEO		
Email:	John.Regan@erc.ie		
For and on behalf of:	The Educational Research Centre		

Table 19.2

Data Protection Officers Statement

This Statement is separate to the Data Sharing Agreement. It is required by law under section 55(1)(d) of the Data Sharing and Governance Act 2019. The Data Protection Officers in each proposed Party must sign and complete this statement before the Data Sharing Agreement is submitted to the Data Governance Unit for Public Consultation and again at execution stage. This statement will be published on a public website.

The Data Protection Officers in each proposed Party to this Data Sharing Agreement must ensure that they:

i. have reviewed the proposed agreement, and
ii. are satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law,
iii. are satisfied that the agreement is consistent with Article 5(1) of the GDPR

The Parties hereby agree to their obligations pursuant to this Data Sharing Agreement for the transfer of personal data as described in this Data Sharing Agreement.

Lead Agency DPO Statement

LEAD AGENCY DATA PROTECTION OFFICERS STATEMENT			
I have reviewed the proposed agreement			☒
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:	Tara Carton	Date:	Nov 23, 2023
Print Name:	Tara Carton		
Position:	Data Protection Officer		
Email:	dpo@education.gov.ie		
For and on behalf of:	Department of Education		

Table 20.1

Other Party/Parties DPO Statement

OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			☒
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:	Damian Downes Damian Downes (Nov 23, 2023 14:08 GMT)	Date:	Nov 23, 2023
Print Name:	Damian Downes		
Position:	Data Protection Officer		
Email:	Data.Protection@erc.ie Damian.downes@erc.ie		
For and on behalf of:	The Educational Research Centre		

Table 20.2