Data Protection Impact Assessment (DPIA)

A Systematic and Comprehensive Analysis of the Personal Data Processing Activities currently engaged in by the Anti Bullying Research & Resource Centre (ABC) in the context of Research Activities

This is a record of a DPIA process and outcome for ABC. It follows the methodology set out in the Data Protection Commission’s guidance and takes account of the criteria for an acceptable DPIA set out in European guidelines.

Preparation Period: January – May 2020
Date considered by DCU DPO: 27th May 2020
Approved by: Noel Prior
Next Review Date: May 2023
# Table of Contents

**Introduction** .................................................................................................................. 3

**Stage 1 - Description and Context of ABC Research Projects** ........................................ 3

1.1 The Anti-Bullying Centre .............................................................................................. 4
1.2 Overview of the Processing Activities .......................................................................... 5-6
1.3 Research Projects ......................................................................................................... 7
1.4 Information Flows .......................................................................................................... 8-9
1.5 Personal Data Security Schedule (PDSS) ..................................................................... 9-10
1.6 Technical Aspects of Data Collection, Storage and Processing ..................................... 10-11
1.7 Technical Data Security and Data Management Measures .......................................... 11

**Stage 2 - Is a DPIA mandatory and is the processing likely to result in “High Risk”** ........... 12

2.1 Does ABC Research involve the processing of personal data? ..................................... 12-13
2.2 Are the processing activities considered “High Risk”? ................................................. 13-15
2.3 Mandatory DPIA ........................................................................................................... 15-17
2.4 Why is a DPIA being conducted by ABC at this time? .................................................. 17

**Stage 3 – Assessment of Necessity and Proportionality** ................................................... 18

3.1 Purpose of ABC Research related processing .................................................................. 18
3.2 Benefits of ABC Research .............................................................................................. 18-19
3.3 The Lawful Basis of ABC Processing .............................................................................. 19
3.4 Relationship with Stakeholders ...................................................................................... 20
3.5 GDPR considerations applicable to Scientific Research Benefits .................................. 20-21
3.6 “Preliminary Opinion” on Data Protection & Scientific Research ................................. 21-22
3.7 Can ABC Activities be regarded as “Health Research”? ................................................ 22
3.8 Assessment of Necessity and Proportionality of ABC Processing ................................. 23

**Stage 4 - Identifying Data Protection Risks** ................................................................... 24

4.1 Risk Based Approach ..................................................................................................... 24
4.2 Description of ABC Research Methodology & Governance ......................................... 25
4.3 Identification of Data Protection and Related Risks ....................................................... 25-26
4.4 Compliance with the GDPR Principles ......................................................................... 27

**Stage 5 – Mitigation Measures** ...................................................................................... 28

5.1 Measures in place to reduce or eliminate risks identified .............................................. 29-30

**Stage 6 - Sign off and Recording the DPIA Outcomes** ................................................ 31

**Stage 7 - Integrating the DPIA Outcomes into ABC Culture** .......................................... 32
1. Introduction

iTrust Ethics (iTE) has been engaged by the Anti Bullying Centre (ABC) in DCU to conduct a review of its data processing practices and compliance with the General Data Protection Regulation (GDPR) by:

- Conducting a Data Privacy Impact Assessment (DPIA)
- Developing an action plan to improve privacy maturity

A DPIA is a means of systematically and comprehensively analysing the personal data processing activities which a controller is engaged in or plans to undertake. It helps to identify and minimise data protection risks and acts as an accountability tool by creating a compliance mechanism for ensuring that the privacy rights of individuals are upheld.

Articles 35 & 36 of the GDPR outline the requirements to consider when completing a DPIA. A DPIA is mandatory for any processing that is likely to result in a high risk to individuals and also in some specified types of activity which have been identified by the Data Protection Commission. Even though the research activities at ABC have been ongoing for some time, the undertaking of a DPIA at this point is considered the most appropriate methodology to allow for a contextual examination of its compliance procedures. It also facilitates an informed and structured approach in identifying risks and implementing mitigation measures.

This completed DPIA will serve as a record of the approach and rationale adopted by ABC and demonstrates compliance with the GDPR provisions to the greatest degree possible.

The review was conducted between January and May 2020 and involved inter alia, gaining an understanding of the data collected, mapping the data flows, assisting in the preparation of a Data Protection Impact Assessment (DPIA) and setting out risk mitigation measures, where relevant. The detail in the DPIA is the output of numerous face to face interviews and follow-up correspondence with ABC leadership and research staff during the review period.
This DPIA should be considered in conjunction with the accompanying action plan to improve privacy maturity at ABC and the pre-existing comprehensive overarching data protection policies in place at Dublin City University.

**STAGE 1 – Description and Context of ABC Research Activities**

This section sets out the nature, scope and context of the processing activities conducted by ABC. It describes the type of personal data that are used as part of ABC’s research and how ABC collects, stores, uses and deletes personal data and who has access to it. The aim of this step is to set out the categories of data that are used as part of the ABC research projects at each step along the process. This is important in identifying the data privacy risks which may be posed and the means that can be used to mitigate those risks.

**1.1 The Anti Bullying Centre (ABC)**

The National Anti Bullying Research and Resource Centre (ABC) is a university designated research centre located in the Dublin City University (DCU). Researchers at ABC undertake research on school bullying, workplace bullying, homophobic bullying, and cyberbullying. ABC leads the field of research, resource development and training in bullying in Ireland and is an internationally recognised centre of excellence in bullying research. The centre’s activities are primarily funded by donors along with support from state agencies and the EU.

ABC research and associated work involves studying the multi-factored causes of bullying and translating its research findings into resources and training to tackle the issue. In 2019 the centre hosted the World Anti-Bullying Forum – a gathering of worldwide experts, educators, parents, and policy makers to discuss and share ideas on methods to tackle bullying, cyberbullying and online safety. The aims of ABC are:

- To conduct research into the multi-level and multi-factorial nature of bullying behaviour (including cyberbullying)
- The creation of greater awareness and understanding of bullying behaviour
• The promotion of ways and means by which bullying behaviour may be prevented or reduced
• To support the National Action Plan on Bullying (2013)\(^1\).

1.2 Overview of the Processing Activities conducted by ABC

The work of ABC has two distinct but related aspects:

**Research** on school bullying, workplace bullying, homophobic bullying, racial/ethnic bullying victimisation, and cyberbullying. This activity is conducted via surveys, questionnaires, interviews and interaction with focus groups. One project, which has not yet commenced, will involve collaboration with computational scientists on developing natural language processing-based tools for addressing bullying on social media platforms proactively. This work will involve working with fully anonymised datasets.

**Translating research findings into resources and training** to tackle bullying – this is achieved mainly through the ABC website and delivery of training in schools, workplaces and the provision of conferences and seminars.

The following examples are outlined to describe the nature of the processing involved:

**ABC Research – Example 1**

A current research project - “Transnational Collaboration on Bullying, Migration and Integration at School Level” (TRIBES) – was highlighted by research staff to illustrate the type of work / processing involved. It is funded by the EU Commission and has received ethical approval from DCU. As part of this project there is a code which identifies the school / institution to which the responder is attached. This facilitates general feedback to the school / institution from ABC. ABC has a practice that feedback will only be given if more than 30 participants from the particular school have responded.

No personal data is collected from the survey participants and there is no means, technical or otherwise of identifying them either directly or indirectly. Assurances were given to ABC by

“SurveyGizmo” – the IT company providing the IT interview platform – that it does not collect IP addresses or other related data regarding responders.

At the time of preparing this DPIA (May 2020), ABC was transitioning from Survey Gizmo to Qualtrics – a platform, which is regarded as best in class, with secure data centres, access controls, cloud infrastructure, high-end firewalls and network security.

**ABC Research – Example 2**

A second example of a research project which is currently being prepared, involves university students. The following points were made in respect of this project:

- Approximately 230,000 students are in the third level education category
- Project has the backing of the Higher Education Authority (HEA)
- Surveys will be anonymous, apart from being able to identify the university to which the respondent is attached
- All participants will be over 18 years and survey will be conducted on-line

**ABC Resourcing – Example 3**

A contact phone number for ABC is displayed on the centre’s website. This is mainly to facilitate schools / institutions or individuals making contact regarding queries on policies and/or participation in projects or training. Occasionally, parents or children phone ABC highlighting a personal experience and seeking advice/guidance. Typically, such calls are answered in the first instance by the ABC secretary and then dealt with by a researcher. Since 2019 one designated researcher, with the appropriate skillset, has responsibility to engage with callers. **This is to ensure continuity of response and minimal sharing of information.** If the designated researcher is unavailable, the secretary records details (identities / contact numbers or email addresses) of the contacting individuals and nature of the query, to facilitate a call back when the researcher is available.

It is accepted at ABC that this aspect of its work involves the processing of personal data. It is further acknowledged that the details recorded may in some limited circumstances constitute sensitive or special category data as defined by the GDPR. The issue of sensitive or special category data usually arises on occasions where parents or children discuss their personal
experiences of bullying and/or its perceived causes (e.g. ethnicity, sexual orientation etc.) or the psychological implications and consequences (depression, anxiety). There has always been a practice at ABC of limiting to the minimum, the number of staff engaging with such callers, the amount of data recorded and its duration of retention.

During the preparation of this DPIA, the processing of this data was considered an area of potential high risk that needed to be mitigated. This issue has been considered in detail and a standardised policy regarding the collection, storage, sharing and deletion of the data, has now been developed. Adherence to the procedures in the policy, will mitigate the risks involved and ensure compliance with GDPR obligations.

1.3 Research Projects

The following specific research projects are being conducted by ABC at the time of writing (May 2020):

1) "BReaThe" - anonymous online survey dataset
2) "FUSE" - anonymous online survey dataset
3) Gifted Children Bullying Prevalence - anonymous online survey dataset
4) Bullying in Higher Education - anonymous online survey dataset
5) TRIBES, “Transnational Collaboration on Bullying, Migration and Integration at School Level” - anonymous qualitative and online survey dataset
6) GEM - Gender, Equality Matters - anonymous survey dataset
7) SEXED - Investigating Online Sexual Harassment and Exploitation project - anonymous online survey data
8) E-Care - Promoting Empathy in the Workplace - anonymous online survey data
9) Cyberbullying in Irish Youth - anonymous online survey data
10) Follow up Telephone Interaction (referred to as Telephone Log in PDSS)

11) Co-designing with Children: A rights-based approach to fighting bullying (project is funded by Facebook). It involves qualitative research with children (focus groups and in-depth interviews which has gone through the full committee review by the DCU Research Ethics Committee and it has also been reviewed by the DCU Data Protection Unit). The project may also involve using an anonymised dataset provided by Facebook with the purpose of optimising the natural language processing tool
(NLP) that the research team is building. This project is a collaboration between ABC and ADAPT Computational Centre at DCU.

The types of data processed in respect of all the above projects are recorded as normal (i.e. not special category) in the Personal Data Security Schedule (PDSS) - see heading 5 of this section. All of the data is recorded (in PDSS) as being held in electronic format. In nine out of the ten cases (at the time of preparation of the PDSS, project 11 – “codesigning with children” – had not begun), the reason or purpose for processing the data is recorded as “research”. The reason for processing no. 10 – Telephone Log – is recorded as “operational”. The legal basis for processing the data is recorded in the first nine categories as “consent and public interest”, while no. 10 is recorded as “public interest”.

1.4 Information Flows

Research Flow

Figure 1: Research process flow
Resource Flow

ABC Resource Process Flow V1

Figure 2: Resource process flow
1.5 ABC Personal Data Security Schedule (PDSS)

In the course of preparing this DPIA, the existing Personal Data Security Schedule (PDSS) in respect of the processing activities conducted by ABC and which had been commissioned by the DCU Data Protection Officer (DCU, DPO) was considered.

The purpose of the PDSS is: must

a) to list the categories of personal data held or processed
b) to set out the security measures practices and controls to be applied for each category of personal data listed
c) to guide DCU staff, researchers and any other DCU users as to their responsibilities when handling, processing, or interacting with the personal data listed in any way

The PDSS, covers nine of the current ten research projects - the tenth project had not commenced at the time of the preparation of the PDSS. The resourcing activity involving phone interaction with callers is also included in the PDSS (see example 3 outlined above and entry under “phone log” in PDSS). The PDSS is set out in a spreadsheet format, under the following category headings:

1) Schedule reference
2) Type, category, or description of the personal data
3) ‘Normal’ or ‘Special’ (aka Sensitive) personal data
4) Format of the data (electronic / paper / both)
5) Unit's or Team's reason or purpose for processing the data
6) Legal basis for processing the data
7) Fixed responsibility for the security of the data
8) Who may access the data?
9) Who may amend the data?
10) With whom may the data be shared?
11) Safeguards and controls to be applied to the data by unit staff / research team
12) How long is the data to be held/retained?
13) Responsibility for data retention; task is assigned to?
14) Method of disposal for the data
15) Is the data shared outside of DCU?
16) Any other comments?

In conjunction with this DPIA, the accompanying “Action Plan to improve ABC Privacy maturity” recommends that the PDSS be updated to reflect all the current research projects and also any updated data protection considerations arising from this analysis.

1.6 The technical aspects of data collection, storage, and processing

The GDPR places significant obligations on controllers regarding the processing of personal data. Additional safeguards and restrictions are imposed for processing if the data is categorised as “sensitive”.

Article 32(1) provides that “…the Controller and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This includes inter alia as appropriate”

1. The pseudonymisation and encryption of personal data
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
4. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Article 32(2) further provides that the appropriate levels of security should be implemented to take account the levels of risk associated with the processing, “…in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed”

1.7 Technical Data Security and Data Management Measures adopted by ABC
The DCU Information Systems Services (ISS) is responsible for the integration, implementation, and support of technology into the teaching, learning and research activity within the university. They have responsibility for the build and maintenance of the Wan/Lan infrastructure and the management all aspects of ICT security.

Among their key responsibilities are providing strategic planning and technical direction and ensuring any emerging technologies are appropriate and fully secure for DCU before deployment. A critical deliverable for the ISS department is the control and management of data, ensuring robust security measures with regards to warehousing, storage, and access controls.

In the context of organisation, custodianship and access controls, ABC implements, among others, the following ISS policies: Cloud Computing, Information & Communications Technology (ICT) Security, Mobile Computing, Network Connectivity, Password Guidance, and Remote Access Controls.
STAGE 2 – Is a DPIA Mandatory? Is the Processing Likely to result in “High Risk”?

2.1 Does ABC Research involve the processing of Personal Data?

‘Personal data’ as defined under GDPR?

For the purpose of GDPR, ‘personal data’ means;

“any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”^2; 

ABC understands this definition to mean data that relates to living persons from which they can be directly or indirectly identified. Direct identifiability means that identification can be achieved from the data itself, while indirect identifiability means that identification can be made from a combination of data with other available data. Data that has been pseudonymised (with identifiers separated) may still be personal data, depending on whether it is possible to reconnect the identifiers with the dataset. This understanding is taken into account when ABC takes all necessary precautions to ensure that minimal identifiable personal data is processed during research.

‘Processing’ as defined under GDPR?

The definition of processing is also taken into consideration by ABC in the context of its research practices. Processing as defined by GDPR means:

“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

---

^2 As defined under Article 4 (1), GDPR
organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”

While ABC researchers strive to anonymise the participants’ identity as much as possible, it is inevitable that some forms of personal data are processed at different stages. The processing of personal data invariably arises in the following activities:

- Collecting written consents from parents and children
- Recording the ages and gender of the interview participants
- Audio recording of interviews in qualitative research projects

### 2.2 Are the processing activities at ABC considered “High Risk”?

The carrying out of a DPIA is only mandatory where processing is “likely to result in a high risk to the rights and freedoms of natural persons” (GDPR - Article 35) or in respect of processing activity designated by the Data Protection Commission (see section 2.3).

A DPIA is particularly relevant when a new data processing technology is being introduced. In cases where it is not clear whether a DPIA is required, it is recognised good practice that a DPIA is carried out nonetheless as it is considered a useful tool to help controllers comply with data protection law.

In assessing whether ABC processing was likely to result in a high risk, consideration was given to the following criteria, which has been set out by the “Article 29 Working Group” and subsequently endorsed by the European Data Protection Board (EDPB).

<table>
<thead>
<tr>
<th>DPIA Screening Checklist</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evaluation or scoring of personal data</strong> (including profiling and predicting) especially “from aspects concerning the data subject’s</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 As defined under Article 4 (2) GDPR.

4 http://ec.europa.eu/newsroom/document.cfm?doc_id=47711; The Article 29 Working Party was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. It was replaced in 2018 by the European Data protection Board (EDPB).

5 http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
<table>
<thead>
<tr>
<th>DPIA Screening Checklist</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements”</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Automated decision-making with legal or similar significant effects</strong>&lt;br&gt;(Processing with little or no effect on individuals does not match this specific criterion)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Systematic monitoring</strong> including through a publicly accessible place on a large scale</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Sensitive data or data of a highly personal nature</strong> (including special categories of data and criminal data)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Data processed on a large scale;</strong> (the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale: i) The number of data subjects concerned, either as a specific number or as a proportion of the relevant population. ii) The volume of data and/or the range of different data items being processed. iii) The duration, or permanence, of the data processing activity. iv) The geographical extent of the processing activity.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Matching or combining data sets</strong>&lt;br&gt;(for example, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Data concerning vulnerable people</strong> (including children)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Innovative use or applying technological or organisational solutions</strong>&lt;br&gt;(New technology can involve novel forms of data collection and usage, possibly with a high risk to individuals’ rights and freedoms. E.g. combining use of fingerprint and face recognition for improved physical access control)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Data transfer across borders outside the European Union</strong></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Processing preventing data subjects from exercising a right or using a service or contract</strong> (This includes processing performed in a public area that people passing by cannot avoid)</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Table 1: DPIA Screening Checklist
The “Article 29” Working Group guidance is that the more criteria that are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA due to the lower level of risk, and processing operations which meet at least two of these criteria will require a DPIA.

It will be noted that 3 criteria from the checklist of the “Article 29” / European Data Protection Board group, have been identified by ABC in its consideration of areas of processing with potential high risk. It is recognised that the checklist is broad in its scope and is merely an aid to controllers. The 3 criteria in question have been included in the context of exercising an abundance of caution by ABC. The 3 criteria in question are:

- “sensitive data or data of a highly personal nature...” This may arise in circumstances where participants discuss personal experiences of bullying and/or its perceived causes (ethnicity, sexual orientation etc.) or psychological implications and consequences (depression, anxiety)
- “Data processed on a large scale...” is included on the basis that some of the research projects involve a large number of participants, although typically this would be conducted online and in an anonymised format
- “Data concerning vulnerable people (including children)” is included on the basis that a significant amount of ABC research work involves children as participants

It is important that these 3 criteria are considered in the unique setting of research - which is designed to enhance the collective knowledge of parents, educators, employers, policy makers and the public generally, regarding the various facets of bullying.

Against this background, it is clearly evident that the objective is not to exploit children but rather to identify issues that might be adversely affecting them both individually and generally and to highlight effective remedial actions, at policy and operational levels.

2.3 Mandatory DPIA – types of processing designated by DPC

The previous section dealt with advice and guidance at EU level concerning the assessment of “high risk” processing activities. This section deals with the specific areas of processing activity which have been identified by the Irish Data Protection Commission (DPC) as
requiring a DPIA. The DPC, in accordance with GDPR Article 35(4), has determined that a DPIA is mandatory for the following types of processing operations\(^6\) 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):

ABC has considered its processing activities against the DPC list as follows:

<table>
<thead>
<tr>
<th>DPIA Screening Checklist – Mandatory DPIAs as designated by Irish Data protection Commission (DPC) – GDPR Article 35(4)</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does ABC processing involve:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to GDPR Article 6(4).</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Profiling vulnerable persons including children to target marketing or online services at such persons.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Systematically monitoring, tracking or observing individuals’ location or behaviour.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Profiling individuals on a large-scale.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals in combination with any of the other criteria set out in WP29 DPIA Guidelines.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for difference purposes or by different controllers.</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

---

Large scale processing of personal data where the Data Protection Act 2018 requires “suitable and specific measures” to be taken in order to safeguard the fundamental rights and freedoms of individuals.

Table 2: DPIA Screening Checklist

It is noted that in many cases the criteria in the DPC check list is more defined and qualified than the EU – EDPB criteria which are broader in scope. For instance, the “use of personal data on a large-scale...”, is qualified by the insertion of “… for a purpose(s) other than that for which it was initially collected pursuant to GDPR Article 6(4)”. Also, the reference to “Profiling vulnerable persons including children” is qualified by the inclusion of “…to target marketing or online services at such persons”.

The type of processing conducted by ABC does not fit any of the criteria identified by the DPC as requiring a mandatory DPIA.

2.4 Why is a DPIA being conducted by ABC at this time?

While DPIAs are usually carried out prior to the processing being undertaken, preferably at design stage, it is felt that there are certain advantages in conducting a DPIA of ABC’s activities at this stage when there is a more developed understanding of the processing activities and the identification of potential risks involved are clearer.

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- “a description of the envisaged processing operations and the purposes of the processing”
- “an assessment of the necessity and proportionality of the processing”
- “as assessment of the risks to the rights and freedoms of data subjects”
- “the measures envisaged to:
  - address the risks”.
- “demonstrate compliance with this Regulation”

---

7 See Articles 35(1) and 35(10), and Recitals 90 and 93 GDPR
3.1 Purpose of ABC Research related processing

Dublin City University (DCU) was designated a university by virtue of the passing into law of the Dublin City University Act 1989\(^8\) (the 1989 Act). The Universities Act, 1997\(^9\) (the 1997 Act) sets out the current legal basis for the operation of the Irish university system.

The 1997 Act outlines the objectives and functions of a University, the structure and role of governing authorities, staffing arrangements, composition, and role of the Academic Council, etc. Section 12 of the Universities act, 1997 outlines the objectives of a university, which include - to advance knowledge through teaching, scholarly research and scientific investigation, to promote learning in its student body and in society generally,

Section 13(1) states that it is the function of a university to “do all things necessary and expedient in accordance with [the University Act] to further the objects and development of the university”.

3.2 Benefits of Research

ABC conducts genuine research within a legislative and ethical framework which greatly adds to the collective knowledge of parents, educators, employers, policy makers and the public generally, regarding the various facets of bullying and its consequences. This research is spearheading the development of next-generation responses to bullying and related issues.

The breadth of ABC’s research expertise is unique globally and the centre’s structure supports collaborative innovation with external partners such as workplaces, schools, charities, and other organisations.

---


ABC research expertise is recognised internally (Ireland) and externally (Europe and globally). It has attracted research funding from Irish state agencies, the EU and global technology companies.

3.3 The Lawful Basis of ABC Processing

Article 6(1)(e) GDPR sets out one of the legal bases for processing as ... “Processing is necessary for the performance of a task carried out in the public interest…….” Article 6(3) GDPR also sets out that where processing is based on this legal basis, it should be grounded on EU or national law, which meets an objective or public interest and is proportionate and legitimate to the aim pursued.

DCU’s status as a university and its mandate and obligation to – ......to advance knowledge through teaching, scholarly research and scientific investigation, to promote learning in its student body and in society generally, and.....do all things necessary and expedient in accordance with [the University Act] to further the objects and development of the university”, provide a legal basis for DCU and by extension ABC, for performing a task in the public interest by discharging its statutory functions to conduct research.

- Necessity, Proportionality, and Minimisation

Whilst relying upon this legal basis (Public Interest Task), ABC has made every effort to ensure that the processing of the personal data of research participants is confined to what is absolutely necessary. Each research project is considered on its individual merits and all research undertaken is governed by the general guiding principle that processing is conducted in a targeted, reasonable, and proportionate manner.

- Children’s Consent

The GDPR contains several specific protections for children’s data protection rights. While ABC relies on the legal basis of public interest task as the legal basis for conducting research, it also incorporates a “double consent” into its procedures as a further ethical and procedural safeguard, in respect of children participants. This involves getting the consent of both the child and its parent or legal guardian, before any research related interaction takes place. Due to the
fact that research is conducted in a controlled environment through schools, ABC is in a position to make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child. The consent forms are stored in a secure cabinet at ABC.

3.4 Relationship with Stakeholders

ABC has a long-established relationship of trust with school principals and teachers through providing advice, guidance and training in anti-bullying research and education. In September 2019, as a continuing development of this relationship, ABC initiated the second phase of project FUSE, a research based programme to train teachers in how to tackle bullying both online and offline. The programme, supported by Facebook, is grounded in Irish and international best practice research, consisting of an in-person training session, online workshops and projects aimed at second year junior cycle students across Ireland.

The training contains six modules, including bullying, cyber bullying, and online safety with a range of resources available to teachers to educate them on how to deal with the scenarios that are likely to occur within the classroom, the school and online. This programme is designed to create champions within each post primary school in Ireland who can then peer train other teachers and parents, in how best to tackle a range of online and offline bullying issues.

3.5 GDPR considerations applicable to Scientific Research

Article 89 of the GDPR provides for flexibility in the obligations on controllers and an emphasis on safeguards and accountability; -

*Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.*
Section 42, Data Protection Act 2018 effectively repeats the contents of Article 89 and confirms that personal data and special categories of data may be processed for these purposes, subject to such processing respecting the principle of data minimisation, and where identification of data subjects is no longer required, the processing should be carried out in a manner which does not permit such identification.

ABC acknowledges the obligations imposed by the GDPR and section 42 of the 2018 Act and adopts a policy of processing the least amount of personal data required to achieve the research objective.

3.6 “Preliminary Opinion” on Data Protection & Scientific Research - Issued by European Data Protection Supervisor, 6th January 2020

There is little by way of guidance or precedent relating to scientific research and the practical application of GDPR provisions. A recent “Preliminary Opinion” from the European Data protection Supervisor (EDPS)\(^\text{10}\) is therefore useful to consider in the context of conducting this DPIA into ABC’s research programmes. An important acknowledgement in the “opinion” is that “… Scientific research depends on the exchange of ideas, knowledge and information”. The following other references in the EDPS document are considered pertinent to ABC circumstances and are summarised in the table below:

<table>
<thead>
<tr>
<th>EDPS “Preliminary Opinion” References</th>
<th>Relevance to ABC</th>
</tr>
</thead>
<tbody>
<tr>
<td>The GDPR contains; -</td>
<td>ABC research work fulfils the criteria of genuine research; operating within an ethical framework; and with the objective of growing society’s collective knowledge.</td>
</tr>
<tr>
<td>a special regime affording a degree of flexibility for genuine research projects that</td>
<td></td>
</tr>
<tr>
<td>o operate within an ethical framework and</td>
<td></td>
</tr>
<tr>
<td>o aim to grow society’s collective knowledge and wellbeing.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>EDPS “Preliminary Opinion” References</strong></th>
<th><strong>Relevance to ABC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private sector research V traditional academic research</strong> is blurrier than ever,</td>
<td>ABC research work can be rightly defined as “traditional academic research”.</td>
</tr>
<tr>
<td><strong>Health science, medical research and clinical trials generally take place within an established framework of professional ethical standards.</strong></td>
<td>ABC research is not considered to encompass “health science” or “health research”.</td>
</tr>
<tr>
<td><strong>The special regime applies the usual principles such as lawfulness, purpose limitation and data subject rights, but permits some derogations from controller obligations.</strong></td>
<td>ABC procedures apply the usual GDPR data protection principles while conducting its research.</td>
</tr>
<tr>
<td><strong>This flexibility is afforded on the assumption that research occurring within a framework of ethical oversight serves, in principle, the public interest.</strong></td>
<td>ABC through its research papers, resourcing, training, and input to government policies has clearly demonstrated a service to the public interest.</td>
</tr>
<tr>
<td><strong>The accountability principle is therefore key, as it requires controllers to assess honestly and manage responsibly the risks inherent in their research projects.</strong></td>
<td>The detail contained in this DPIA clearly demonstrates the informed, honest assessment and management of data protection risks associated with its research.</td>
</tr>
<tr>
<td><strong>'informed consent' may still serve as a safeguard in cases where consent is not appropriate as a data processing legal basis.</strong></td>
<td>ABC uses “double consent” (parent &amp; child) procedure as an ethical and procedural safeguard.</td>
</tr>
</tbody>
</table>

Table 3: EDPS Preliminary Opinion Relevance to ABC

3.7 Can ABC activities be regarded as Health Research?
Even allowing for the broad definition of “health research”\textsuperscript{11}, it is not considered that ABC research work can be regarded as such. However, the issue has been considered in the preparation of this DPIA because if ABC research was to be considered as “health research”, then a third layer (in addition to GDPR & 2018 DPA Act) of data protection rules would apply - the Data Protection Act 2018 (Section 36(2)) (Health Research) regulations 2018 (S.I. No. 314/2018)\textsuperscript{12} - governing health research in Ireland.

3.8 Assessment of the Necessity and Proportionality of the Processing

ABC understands that “Necessity” entails that research related processing should be a reasonable and proportionate method of achieving a given goal, considering the overarching principle of data minimisation. Necessity also requires that personal data should not be processed where there is a more reasonable, proportionate, and less intrusive way to achieve a goal.

ABC is satisfied from its subject matter experience and expertise on anti-bullying research, that there is no less intrusive or equally effective means of conducting its work, other than the methodology which it currently employs.

In asserting that the methodology is strictly necessary, ABC has interpreted this (as per DPC guidance) as meaning that it is not the case that it is simply convenient, potentially useful, or just the standard practice.

The research methodology is considered the most proportionate way of eliciting necessary information from target groups, by a dedicated team of academics, in a strictly controlled environment. Every effort is made to minimise the personal data processed from the research data subjects.

\textsuperscript{11} Section 3.2 (Health Research) regulations 2018 (S.I. No. 314/2018).

STAGE 4 - Analysis of identifying the Data Protection and Related Risks

1. 4.1 Risk Based Approach

A “risk” is a scenario describing an event and its consequences, estimated in terms of likelihood and severity. “Risk management”, on the other hand, can be defined as the coordinated activities to direct and control an organisation with regard to risk. ABC recognises that during its processing activities, there is the potential that the data may be exposed to risks. ABC accepts that it has a responsibility to take steps to ensure that the data is handled legally, securely, efficiently, and effectively. The risk-profile of the personal data which ABC process, is determined according to: the processing operations conducted; the complexity and scale of the processing; the sensitivity of the data; the protection required for the data being processed.

ABC makes stringent efforts to minimise the amount of personal data processed during its research work. ABC acknowledges that due to the sensitive subject matter involved in its research, any inappropriate divulgence of personal data potentially attracts a higher risk rating than the routine personal data that relates the day to day administration of the faculty.

Consequently, when considering the risk profile of the personal data being processed by ABC in the context of its research, consideration is afforded to the tangible harms to individuals that need to be guarded against. In particular cognisance is taken of processing that could give rise to: discrimination, identity theft/fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage.

The involvement of a broad representation of ABC staff in the course of preparing this DPIA and conducting the risk-assessment, has served to enhance awareness and knowledge of their duties and responsibilities regarding data protection considerations. It is envisaged that this will enhance the existing positive culture of compliance in respect of protection of data and will facilitate the practical application of embedding data privacy features into current and future projects.
4.2 Description of ABC Research Methodology and Governance

DCU and by extension, ABC is committed to ensuring the highest standards of integrity in all aspects of research and this commitment is formally expressed through the codes and policies which are specific to research integrity. These policies include:

- DCU Code of Good Research Practice
- DCU Code of Practice on Authorship
- DCU Policy for Responding to Allegations of Research Misconduct
- DCU Position Statement on Open Access to Research Publications

In order to promote best practice in responsible research behaviour, DCU provides training on research integrity. This includes online research integrity modules tailored for early stage researchers and experienced researchers, plus a research integrity training programme targeted at graduate research students. Research integrity is also a key component in the induction of staff and research students. Presentations and other on-line resources are made available to the DCU research community via the research support section of its website.

ABC research projects are first considered by the DCU Research Ethics Committee (REC), which exists to promote the highest ethical standards in all research at DCU involving human participants or animal subjects. If the DCU REC approves a research project, it is then subject to the various policies applicable to research and the legal data protection obligations imposed by regulation (GDPR) and national legislation (2018 Data Protection Act).

4.3 Identification of Potential Data Protection and Related Risks

In the context of preparing this DPIA, ABC prepared a data protection risk register to describe the risks associated with its research projects and assess their likelihood and impact. This risk register is intended to act as a record of the potential risk exposure to data during the life cycle of individual research projects. The register should be read in conjunction with the ABC
Personal Data Security Schedule (PDSS) and the risk mitigation measures outlined in section 5 of this DPIA.

### Data Protection and Potential Risk - Scoring Matrix - (Low 1 – 5 High)

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Risk</th>
<th>Probability</th>
<th>Impact</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data leakage, unauthorised or inappropriate use of data.</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>Cyber Security: ‘hacking’ and attacks aimed at theft of IP (leading to reputational damage, compromised systems, and loss of personal data).</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>Data Breach associated with storage of hard copies of research papers/ Questionnaires.</td>
<td>3</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>4</td>
<td>Breach of GDPR associated with deviation from methodologies for the management of research projects.</td>
<td>3</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>Storage of personal data on local PC’s/Laptops</td>
<td>3</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>6</td>
<td>Personal data being used in a manner or for a purpose not anticipated by the research participant due to the evolution (function creep) in the nature of the project.</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>Vulnerable individuals about whom sensitive data is kept, might be affected to a high degree by inappropriate disclosure of personal data. (research records &amp; “Call Logs”)</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 4: Risk Score

The assessment of risk (Very Low, Low, Medium, High, Very High) is determined by comparing the Risk Score in Table 4 against the Risk Rating Matrix at Table 5 below:

<table>
<thead>
<tr>
<th>Probability</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very low (1)</td>
</tr>
<tr>
<td>Very high (5)</td>
<td>5</td>
</tr>
<tr>
<td>High (4)</td>
<td>4</td>
</tr>
<tr>
<td>Medium (3)</td>
<td>3</td>
</tr>
<tr>
<td>Low (2)</td>
<td>2</td>
</tr>
<tr>
<td>Very low (1)</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 5: Risk Rating Matrix
The maintaining and updating of this register acts as a record of the identified risks, together with an assessment of their likely occurrence and potential impact. It will be treated as a “living document” and updated as projects progress, to reflect any new identified risks.

### 4.4 ABC Compliance with GDPR Principles

The GDPR sets down 6 principles for collection, use, sharing and storage of personal information data processing: The table below shows how ABC performs against these principles.

<table>
<thead>
<tr>
<th>GDPR Principles</th>
<th>ABC Compliance</th>
</tr>
</thead>
</table>
| **Lawfulness, Fairness and Transparency** | Processed lawfully, fairly and in a transparent manner  
  All Research is examined by DCU Ethical Committee to ensure that project fulfils the research mandate of the university and the lawful basis of “Task in the Public Interest”.  
  Clear and ‘age appropriate’ explanation to participants concerning the nature of the research and the use to be made of their personal data.  
  “Double consent” used in respect of child participants.                                                                                     |
| **Purpose Limitation**                 | Collected for specified, explicit and legitimate purposes  
  Data used exclusively for the purpose of the project which is explained at the outset.  
  Policy guidelines and procedures to prevent deviation from purpose and prevent “function creep”.                                                                 |
| **Data Minimisation**                  | Adequate, relevant and limited to what is necessary  
  Standard research templates utilised which contain minimum personal data required from participant. Adherence to standard questions is vital for research integrity and also ensures a consistent approach to data minimisation. |
| **Accuracy, and where necessary up to date** | ABC members are subject to academic oversight procedures and are experienced at demonstrating accuracy of data.                                                                                                 |
GDPR Principles | ABC Compliance
--- | ---
**Storage Limitation**
Retained only for as long as is necessary | Data is retained in accordance with academic requirements for proving integrity of research methodology and output.

**Integrity and Confidentiality** | Projects are approved by ethical board.
Strict controls regarding sharing of and access to personal data of participants.

Table 6: ABC Compliance with GDPR Principles

**STAGE 5 – Mitigation Measures**

*Identifying and Evaluating the Data Protection Solutions to Reduce or Eliminate the Risks*

This stage follows on from the identification of data protection risks at stage 4, with the aim of minimising any data privacy risks, insofar as possible. Whilst acknowledging that it is not possible to eliminate data protection risks completely, the objective is to ensure that any remaining risks are proportionate.

ABC is satisfied that it has mitigated all identified risks, including potential high risks, to the greatest extent possible. The risk mitigation measures and the assessed effect on the risks, are outlined in Table 7 below.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Measures to reduce or eliminate risk</th>
<th>Effect on risk</th>
<th>Residual risk</th>
<th>Measures approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Data leakage, unauthorised or inappropriate use of data</td>
<td>Data Protection Policy and Record Management Policy in place and guidance is available to staff.</td>
<td>R</td>
<td>L</td>
<td>Measures In Place</td>
</tr>
<tr>
<td></td>
<td>Comprehensive controls over access, data flows, inputs and outputs are formally documented and authorised.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Cyber Security: ‘hacking’ and attacks aimed at theft of IP (leading to reputational damage, compromised systems and data and loss of IP).</td>
<td>Physical access controls, firewalls. Comprehensive policies established.</td>
<td>R</td>
<td>M</td>
<td>Measures In Place</td>
</tr>
<tr>
<td></td>
<td>Regular offsite backups completed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Awareness training for all staff.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Laptop encryption monitored.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security strategy and patch management in place.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Data Breach associated with storage of hard copies of research papers/ Questionnaires</td>
<td>Secure file storage for hard copies with appropriate governance and access controls.</td>
<td>R</td>
<td>L</td>
<td>Measures In Place</td>
</tr>
<tr>
<td>Table 7</td>
<td>Measures in place to reduce or eliminate risks identified in stage 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Measures to reduce or eliminate risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Effect on risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Residual risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Measures approved</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eliminated Reduced Accepted High Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes/No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Breach of GDPR associated with non-adherence to methodologies for the management of research projects</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Documented procedures and methodologies on the management of research projects with specific consideration on the collection and management of personal data.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R  L  Measures in Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Storage of personal data on local PC’s/Laptops</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy preventing the storing of personal/sensitive data on local drives on PC’s or Laptops.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy preventing the downloading of data to external drives.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All personal data must be stored securely in the cloud with appropriate access controls.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R  M  Measures in Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table 7</td>
<td>Measures in place to reduce or eliminate risks identified in stage 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Measures to reduce or eliminate risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Effect on risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Residual risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Measures approved</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Personal data being used in a manner or for a purpose not anticipated by the research participant due to the evolution (function creep) in the nature of the project</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transparency and clear policy guidelines at the outset concerning nature and scope of research projects. Reviews during project to prevent deviation.</td>
<td>R</td>
<td>L</td>
<td>Measures In Place</td>
</tr>
<tr>
<td>7.</td>
<td>Vulnerable individuals or individuals about whom sensitive data is kept, might be affected to a high degree by inappropriate disclosure of personal data (Telephone Call Logs).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy dedicated to “Telephone Call” data. Strict access controls. Secure storage for electronic and paper records.</td>
<td>R</td>
<td>M</td>
<td>Measures In Place</td>
</tr>
</tbody>
</table>

Table 7: ABC Risk Mitigation
STAGE 6 – Sign Off and Recording the DPIA Outcomes

The primary aim of conducting this DPIA is to identify and minimise the data protection risks involved in ABC research projects. It also serves as a record of the methodology and rationale employed and demonstrates compliance with data protection obligations, in line with the GDPR principle of accountability. It will also facilitate the ongoing review of the effectiveness of the risk mitigation measures in place.

Sign off and record of outcomes

<table>
<thead>
<tr>
<th>Item</th>
<th>Name/position/date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measures approved by:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Residual risks approved by:</td>
<td></td>
<td>No residual high risk remaining.</td>
</tr>
<tr>
<td>DPO views sought: [GDPR - Article 35(2)]</td>
<td>Yes</td>
<td>N/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This DPIA was reviewed by staff of the DPU on 27/5/20 and the DPO has given his approval for the control measures outlined by management</td>
</tr>
</tbody>
</table>

Summary of DPO advice: To follow the controls already documented in this DPIA.

DPO advice accepted or overruled by: If overruled, Give rationale / explanation

Comments:
This DPIA shall be interpreted as a “draft” until it has been considered by the DCU DPO and signed off by ABC management.

When approved, the DPIA shall be considered in conjunction with:

- The accompanying Action Plan to improve privacy maturity at ABC
- The Policy for the Handling of Information, arising from persons making telephone contact with the Anti Bullying Centre (ABC)
- The updated ABC “Personal Data Security Schedule” (PDSS)
- The comprehensive overarching DCU Data Protection Policies

ABC staff will continue to keep data protection issues under review to ensure that the mitigation measures are having the intended effect. Additionally, if the research projects aim or methodologies change or expand in the future, it is recognised that it will be necessary to consider the adequacy of existing arrangements.

Copies of this DPIA, the Action Plan for improving maturity & “Telephone Log” policy, will be available in electronic format to all ABC staff working on research projects or having any associated data protection responsibilities.