The Active Learning Trust

DATA PROTECTION IMPACT ASSESSMENT (DPIA) POLICY AND PROCEDURE

This policy is reviewed every three years

History of Document

Issue No	Author/Owner	Date Reviewed	Date Approved by Trust Board	Comments
1	DPO	November 2018	13 December 2018	1st formal issue
2	DPO	February 2019	14 February 2019	Inclusion of 2.4 where DPIAs are reported

1. INTRODUCTION

1.1 This Data Protection Impact Assessment Policy ("policy") defines the Active Learning Trust's ("Trust") expected practice to be undertaken when completing Data Protection Impact Assessments ("DPIAs"). The policy is one of the Trust's Information Governance suite of policies.

1.2 DPIAs are an integral part of taking a 'privacy by design' approach and are a way for organisations to systematically and comprehensively analyse processing and help identify and minimise data protection risks.

1.3 DPIAs are important tools for accountability as they help data controllers not only to comply with requirements of the General Data Protection Regulation ("GDPR"), but also to demonstrate that appropriate measures have been taken to ensure compliance with GDPR. In other words, a DPIA is a process for building and demonstrating compliance.

1.4 This policy and procedure is based on comprehensive guidance produced by the Information Commissioner's Office ("ICO"), which can be accessed at:

ICO DPIA Guidance

2. Responsibility for completing DPIAs

2.1 The Trust expects its Data Protection Officer ("DPO") to work with a school's project lead to complete a DPIA.

2.2 The DPO will maintain a register of DPIAs undertaken and ensure that DPIAs are reviewed as a minimum every two years unless changes to processes have been identified by either the DPO or project lead.

2.3 DPIAs will be signed off by the Finance and Operations Director until schools are confident in the completion of DPIAs without the DPO's assistance. When this occurs, the DPO will solely sign off the DPIAs.

2.4 The DPO will report on the status of completion of DPIAs to the Information Governance Working Group and within the Data Protection and Compliance Report to the Trust Board.

3. Requirement for a DPIA

3.1 The GDPR records that a DPIA **must** be undertaken where processing is likely to result in a "high risk" to the rights and freedoms of natural persons such as:

3.1.1 use of systematic and extensive profiling with significant effects;

3.1.2 process of special category or criminal offence data on a large scale; or

3.1.3 systematically monitoring of publicly accessible places on a large scale.

3.2 A DPIA has to be performed **before** the processing/project begins.

3.3 The ICO also requires an organisation to produce a DPIA if it plans to:

3.3.1 use new technologies;

3.3.2 use profiling or special category data to decide on access to services;

3.3.3 profile individuals on a large scale;

3.3.4 process biometric data;

3.3.5 process genetic data;

3.3.6 match data or combine datasets from different sources;

3.3.7 collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

3.3.8 track individuals' location or behaviour;

3.3.9 profile children or target marketing or online services at them; or

3.3.10 process data that might endanger the individual's physical health or safety in the event of a security breach.

3.4 The ICO requires organisations to consider if a DPIA is required if there are plans to carry out:

3.4.1 Evaluation or scoring;

3.4.2 Automated decision-making with significant effects;

3.4.3 Systematic processing of sensitive data or data of a highly personal nature;

3.4.4 Processing on a large scale;

3.4.5 Processing of data concerning vulnerable data subjects;

3.4.6 Innovative technological or organisational solutions; or

3.4.7 Processing involving preventing data subjects from exercising a right or using a service or contract.

3.5 DPIAs should be embedded into an organisation's processes with the outcome influencing plans. A DPIA is not a one-off exercise and should be seen as an ongoing process and regularly reviewed. The procedure to be followed is held at appendix I.

4. Initial Screening

4.1 A DPIA initial screening form (refer appendix II) must initially be completed by a school's project lead responsible for delivering the proposed change. The purpose of the screening questions is to assess whether a DPIA assessment is required.

4.3 If the answers to the screening questions are "no", the screening process has therefore not identified any DPIA concerns and the process is considered as complete. If a response to any of the questions is "yes", then a DPIA must be undertaken.

4.4 In some cases the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

4.5 A DPIA initial screening form must be sent to the DPO for review and authorisation.

5. Steps of a DPIA

5.1 If the outcome of the DPO's review of the DPIA initial screening form is the requirement for a DPIA to be completed (as per appendix II), the DPO will send the form to the project lead for completion as far as possible. The DPO will work with the project lead to complete the form.

5.2 The completion of a DPIA will include eight steps as described below:

5.2.1 Step one - Identification of the need for a DPIA;

5.2.2 Step two - Description of the nature, scope, context and purposes of the processing;

5.2.3 Step three - Consultation process;

5.2.4 Step four - Assess necessity and proportionality;

5.2.5 Step five - Identify and objectively assess compliance risks - through consideration of both the likelihood and severity of any impact on individuals. Broader risks to the rights and freedoms of individuals should also be considered, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or society at large, whether it is physical, material or non material. The checklist reviews the data protection principles.

5.2.6 Step six - Identify measures to mitigate or eliminate high and medium risk through consideration of both the likelihood and severity of any impact on individuals. Implement and integrate these into the project plan. A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified. The ICO is to be consulted before processing, if high risks can not be mitigated.

5.2.7 Step seven - Sign off and record of outcomes. This step requires the recording of the decision-making in the outcome of the DPIA, including any difference of opinion with the Trust's DPO or individuals consulted. The DPIA is to be signed off by the Trust's Director of Finance and Operations – as per point 2.3.

5.2.8 Step eight - Integrate the DPIA outcomes into the project plan. DPIAs to be kept under review and revisited when necessary.

6. Consulting the ICO

6.1 The ICO must be consulted at step six if a DPIA identifies a high risk and an organisation can't take measures to reduce that risk. In such situations, processing can't begin until the ICO has been consulted. The ICO will take generally respond within eight weeks.

7. Review

7.1 This Policy will be reviewed every three years by the Trust Board.

APPENDIX I PROCEDURE

1. DPIA Initial Screening Form

The school's project lead must complete a DPIA Initial Screening Form held at appendix II. It includes questions which will help a decision be made as to whether a DPIA is necessary. Answering "yes" to any of the initial screening questions is in indication that a DPIA would be a useful exercise.

Upon completion, the initial screening form must be sent to the Data Protection Officer ("DPO") for review.

The DPO will review the initial screening form and if it results in a DPIA not being necessary, then the DPO will log this on the register of Initial Screening Forms. No more action required.

If the DPO's review results in a decision that a DPIA must be undertaken she will file the Initial Screening Form in the folder set up for the appropriate DPIA.

2. DPIA Register

The project will be logged on the DPIA register and a folder set up for the DPIA. A number will be allocated to the DPIA.

3. DPIA Form

The DPO will send the DPIA to the project lead who will complete steps 1-3 inclusive of the DPIA form (there may be some questions that can't be answered initially).

Step 1: In this step the following are to be recorded: the need for a DPIA**,** an explanation of what the project or process aims to achieve, the benefits = to the Academy, to individuals and other parties and what type of processing it involves. It may be helpful to refer or link to other documents, such as a project proposal.

Step 2: In this step the following are to be recorded:

A description of the nature of the processing - how will the personal data be collected, used, stored and deleted? What is the source of the data? Will the personal data be shared with anyone? It may be beneficial to refer to a flow diagram or other way of describing data flows. Describe the types of processing identified as likely high risk.

A description of the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will be collected and used? How often? How long will it be kept? How many individuals are affected? What geographical area does it cover?

A description of the context of the processing: what is the nature of the school's relationship with the individuals? How much control will they have? Would they expect the school to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that should be factored in? Is the school signed up to any approved code of conduct or certification scheme (once any have been approved)?

A description of the purposes of the processing: what does the school want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for the school, and more broadly?

Step 3: In this step relevant stakeholders are consulted. A description of when and how individuals' views will be sought must be recorded else a justification must be recorded–why it's not appropriate to do so. Record who else needs to be involved in the school. Who Record whether processors need to be asked to assist. Record whether there is a plan to consult information security experts, or any other experts.

After completing the above, the DPIA form should be returned to the DPO who will undertake a risk assessment through completion of steps 4-6 inclusive.

Step 4: The DPO will assess the necessity and proportionality and describe the compliance and measures.

Step 5: The DPO will Identify and objectively assess risks and record the likelihood of harm (remote, possible or probable); severity of harm (minimal, significant or severe) and overall risk (low, medium or high.)

Step 6: The DPO will identify additional measures that could be taken to reduce or eliminate risks identified as medium or high risk in step 5.

4. Approval of the DPIA

Step 7: The DPO will consider whether to approve the measures and will record any actions that require to be integrated back into the project plan, with date and responsibility for completion.

The DPO will consider the residual risks. If accepting any residual high risk, the DPO will consult the ICO before going ahead.

The DPO will record a summary of her advice on compliance, step 6 measures and whether processing can proceed.

The Director of Finance and Operations will then be required to approve and sign off the DPIA Form.

The DPIA will be kept under review by the DPO/Project Lead and the DPO should also review ongoing compliance with the DPIA.

5. Integrate the DPIA outcomes into the project plan

Step 8 - This step records the DPO must record any DPIA outcomes that need to be integrated into the project plan, the names of persons responsible for such work and completion date.

APPENDIX II DPIA INITIAL SCREENING FORM

Project/Process Name	
Brief outline of the project	
Project Lead	
Date	

SECTION 1: DPIA screening questions

These questions are to help the Academy decide whether the DPIA is necessary. Answering "yes" to any of these questions is in indication that a DPIA would be a useful exercise. Once completed please pass to the Data Protection Officer for review. Some answers may not be known at this time.

Question	Yes	No	Notes
Will the new project/process involve the collection of new information about individuals?			
Will the new project/process compel individuals to provide information about themselves?			
Will information be used about individuals for a purpose that is not already currently used, or in a way not currently used?			
Does the project involve using new technology/software which might be perceived as being privacy intrusive, e.g. biometrics?			
Will there be a trial in software, software downloaded for free which require personal data to be uploaded?			
Will the project result in decisions being made or action being taken against individuals in ways which can have a significant impact on them?			
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? e.g. health records/ criminal records or other information that people would consider to be particularly private?			
Will the project require individuals to be contacted in ways which they may find intrusive?			

SECTION 2: Data Protection Officer – feedback/decision

APPENDIX II DPIA TEMPLATE

Step 1: Identify the need for a DPIA

Explain what the project or process aims to achieve; what benefits will be to the Academy, to individuals and other parties and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why the need for DPIA was identified.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? Will personal data be manually input or feed direct from SIMs?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures.	
What is the lawful basis for processing	
Does the processing actually determine the school's purpose?	
Is there another way to achieve the same outcome?	
How will you prevent function creep?	
How will you ensure data quality and data minimisation	
What information will you give individuals?	
How will you help to support their rights?	
What measures do you take to ensure processors comply?	
How do you safeguard any international transfers?	

Step 5: Identify and assess risks

For each of the following risks – identify the likelihood of harm (remote, possible or probable); severity of harm (minimal, significant or severe) and overall risk (low, medium or high

Risk	Answer and likelihood/severity of harm and overall risk
1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.	
1.1 The purpose of the project/process has not been identified.	
1.2 Conditions for processing have not been established.	
1.3 Individuals have not been told about the use of their personal data.	
1.4 The rights of individuals are unknown.	
1.5 If consent is required, its collection, withholding and withdrawal have not been identified.	
1.6 Personal data may be held outside the EEA?	
1.7 Privacy notices require amendment but haven't been amended	
1.8 Personal information will be passed to third parties and sub processors.	
1.9 There is no data sharing agreement, protocol or contract	
2. Personal data shall be collected for specified, explicit and legitimate purposes	
2.1 The project does not cover all of the purposes for processing personal data.	T
2.2 Potential new purposes have not been identified as the scope of the project expands.	

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed?	
3.1 The information is not of good enough quality for the purposes it will be used.	
4. Which data could not be used without compromising the needs of the project?	
4.1 Personal data is not accurate and not kept up to date	
4.2 Any new software or process does not allow the amendment of data when necessary.	
4.3 The Academy does not ensure the accuracy of data obtained from individuals or other organisations.	
5. Personal data shall be kept in a form which permits identification if data subjects for no longer than is necessary	
5.1 The retention period is not suitable for the personal data being processed.	
5.2 The procured system will not allow deletion of information in line with retention periods.	
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.	
6.1 The new system(s) does not provide protection against any identified security risks.	
6.2 Training and instructions will not be given to staff to operate new systems and keep data secure.	
6.3 Where personal data is held outside the EEA, the security of such meets the ICO's requirements.	

Step 6: Identify measures to reduce risk

Identify additional measures that could be taken to reduce or eliminate risks identified as medium or high risk in step 5.

Risk	Options to reduce or eliminate risk. Effect on risk (eliminated reduced accepted); residual risk (low, medium, high); measure approved – yes/no
1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.	
1.1 The purpose of the project/process has not been identified.	
1.2 Conditions for processing have not been established.	
1.3 Individuals have not been told about the use of their personal data.	
1.4 The rights of individuals are unknown.	
1.5 If consent is required, its collection, withholding and withdrawal have not been identified.	
1.6 Personal data may be held outside the EEA?	
1.7 Privacy notices require amendment but haven't been amended	
1.8 Personal information will be passed to third parties and sub processors.	
1.9 The us no data sharing agreement, protocol or contract	
2. Personal data shall be collected for specified, explicit and legitimate purposes	
2.1 The project does not cover all of the purposes for processing personal data.	

2.2 Potential new purposes have not been identified as the scope of the project expands.	
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed?	
3.1 The information is not of good enough quality for the purposes it will be used.	
4. Which data could not be used without compromising the needs of the project?	
4.1 Personal data is not accurate and not kept up to date	
4.2 Any new software or process does not allow the amendment of data when necessary.	
4.3 The Academy does not ensure the accuracy of data obtained from individuals or other organisations.	
5. Personal data shall be kept in a form which permits identification if data subjects for no longer than is necessary	
5.1 The retention period is not suitable for the personal data being processed.	
5.2 The procured system will not allow deletion of information in line with retention periods.	
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.	
6.1 The new system(s) does not provide protection against any identified security risks.	
6.2 Training and instructions will not be given to staff to operate new systems and keep data secure.	
6.3 Where personal data is held outside the EEA, the security of such meets the ICO's requirements.	

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
Summary of DPO advice - DPO should advise on compliance, step 6 measures and whether processing can proceed		
Second Signature – Director of Finance and Operations:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Step 8: Integrate the DPIA outcomes into the project plan

This step records the DPIA outcomes that need to be integrated into the project plan and the names of persons responsible for such work.

Actions to be taken	Date for completion of actions	By whom