Academies Enterprise Trust
To make our best better

Data Protection Impact Assessment (DPIA)

Before completing this Data Protection Impact Assessment (**DPIA**) please read the Data Protection Impact Assessment Policy, which provides an overview of the DPIA process. Please also read the guidance notes set out below.

Guidance notes

Who should complete the questionnaire?

An individual with oversight of the project should be appointed to ensure that the questionnaire is completed. However, input will be required from a number of areas. You will need to consider which business units will need to provide information and circulate the questionnaire to those business units, indicating which questions they need to complete.

Where a third party supplier is involved with the project, the third party supplier should be asked to complete Section A. The information provided by the supplier should be checked by Academies Enterprise Trust (AET) to ensure it is accurate and comprehensive.

What is personal data?

Personal data means any information that relates to a living individual. This will include (amongst others) name and contact details, job-related information (such as salary and performance information) and any financial information we hold about an individual. Personal data also includes opinions about an individual.

What are special categories of personal data?

There is a subset of personal data that is designated as special category personal data. More onerous restrictions are in place in relation to the way that organisations may use special categories of personal data. Special categories of personal data include information about the following:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- biometric data
- genetic data
- sexual life

Information about criminal offences or allegations of criminal offences or proceedings in relation to criminal offences is also subject to more stringent legal requirements. For the purposes of this DPIA, criminal conviction data should be treated like special category personal data.

How to complete Section A

Please provide full and comprehensive answers to each question. Remember that there are no right or wrong answers. The aim of Section A is to obtain a good understanding of how personal data will be impacted by the project.

You are not expected to have identified solutions to all privacy risks at this stage therefore you may need to respond 'Not yet known' or 'To be confirmed' to some questions. Where this is the case, the DPIA process will help to identify appropriate solutions.

If any questions are not applicable, please state N/A.

How to complete Section B

Section B should be completed with assistance from the DPO. The purpose of this Section is to identify any privacy risks to individuals and also any compliance or reputational risks for Academies Enterprise Trust [AET]

How to complete Section C

For each risk identified in Section B an appropriate solution to mitigate or eliminate that risk needs to be identified and documented in Section C. The DPO should review identified solutions to ensure they are adequate.

Where a third party supplier is involved in the project and is required to implement any of the solutions, the relevant solution should be included as a contract requirement for the supplier.

How to complete Section D

Once solutions have been identified Section D should be updated to show the status of implementation of each solution. If there are any risks for which an appropriate solution has not been identified, the DPO must be consulted to advise on the risks of proceeding with the project and/or whether relevant data protection regulators need to be consulted. As solutions are implemented, the table in Section D should be updated to reflect the reduced/eliminated risk.

How to complete Section E

The Trust must be able to demonstrate that personal data used in the project is necessary and proportionate. An analysis of the need to use personal data in order to achieve the objectives of the project should be inserted in Section E.

How to complete Section F

In order for data processing to be lawful, one of the legal bases set out in the data protection legislation must be met. The table in Section F must be completed to identify the relevant legal basis being relied upon. Please note that more than one option may be ticked in this table. In each case further details explaining why the chosen legal basis is applicable must be inserted.

Where should this document be saved?

When completed this document should be saved securely to a designated shared drive folder for the function or academy, and sent to the Data Protection Officer (DPO) at: dataprotection@academiesenterprisetrust.org for audit purposes. The email must include the the following information in the subject line: DPIA, name of Academy/ department and description of assessment.

When should this document be updated?

This document should be updated on a continuous basis until all identified solutions have been implemented. Once all solutions have been identified an appropriate review date should be set to ensure that the solutions are working in practice and to update the solutions if the requirements of the project change over time.

Project Details

[redacted]

Section A: Fact-gathering

1	Please provide an overview of the project, including details of key individuals responsible for delivering the project. ***Guidance:*** *You may insert a project overview document here or provide your own summary description.*
	AS Tracking is an online pastoral assessment system taken by pupils that allows schools to make visible and track every pupil voice informing the holistic approach AET take to pupil development to create better outcomes -detail is here on the website: https://steer.global/en/products/as-tracking Having completed a successful pilot of AS Tracking across 4 AET schools, STEER and AET are working towards a roll out across @20+ schools with a focus on KS4&5 but potentially other KS to be included AS Tracking is owned by STEER - benefits of this system is to support students using pupil voice to diagnose areas or weakness to help support improve their outcomes. STEER Lead: [redacted] AET Lead: [redacted]
2	What personal data will be collected as part of the project and to whom does the personal data relate? ***Guidance:*** *Please list all types of personal data that will be collected e.g. name, address, telephone number, date of birth. Please list of categories of individuals whose personal data will be collected e.g. customers, employees.*
	The provision above the personal data on the STEER system would be as follows: Pupil surname, first name initial, date of birth (although this is generalised on import to 01 for 'dd'), gender, school year Other data fields which are optional are detailed on the document 'How to choose your data fields) STAFF personal data- first and surname, school email addresses and contact phone. See Privacy policy for school staff for further details
3	Is it necessary to use all of the personal data described above? Please remember that the use of personal data must be proportionate and reasonable and that we must take steps to minimise personal data that is collected so far as possible. Please explain below why you consider the collection and use of personal data is necessary and proportionate.
	The AS Tracking assessment will not run without the essential data fields Our essential fields are as follows: DATE OF BIRTH, ANON_NAME CODE, GENDER, SCHOOL YEAR, MIS_PUPIL_ID, PASSWORDS; Our optional additional data fields are as follows: NEW Pupil, boarding status, house name, form group, form tutor, campus, SEND_ flag or status, AEN_flag or status EAL, PUPIL PREMIUM, LOOKED AFTER CHILD, MidYIS_BAND, CAT_BAND, Bursary_Funded, passport nationality, top academic or GIFTED, heavily committed, Safeguarding_Flag, current welfare plan, recently bereaved, ANON_USERNAMES. ADDITIONALLY, school may choose up to three CUSTOM data fields to look at any culturally relevant trends for the setting. The optional data fields provide vital data for the analysis of trends within specific cohorts from the assessment results.
4	Approximately how many individuals are impacted by the project (i.e. whose personal data will be involved)?
	Trial range of 853 students. Potential roll-out to all student & staff = 34,000 Students and 4,000 Staff
5	From where will personal data be collected? Please describe all sources of personal data. ***Guidance:*** *For example, this may include existing databases, directly from individuals themselves, third party sources or a combination of different sources.*
	AET Data Lake will be automatically updated from an SFTP site using CSVs[MIS, safeguarding, SENDCo]
6	On what systems/databases will personal data be stored?
	STEER Platform. Dedicated servers are hosted and managed by Rackspace See Global Information on the host provider-Rackspace for certifications
7	Who will be responsible for inputting personal data into systems?
	Usually the school data manager but I understand that AET will be importing the data centrally. STEER Administrators add L5 and L3 credentials for school staff (see answer to access question below)
8	What checks/processes will be put in place to ensure that personal data is accurate and kept up-to-date?

	The AET Data Manager has full control and responsibility for maintaining the accuracy of the data. We do not currently have an API and so the updates would be manual until that is implemented
9	Who within AET will be able to access the personal data?
	Any academy and central support staff with platform logins. Permission matrix is applied-see below
10	How will this access be authorised?
	Group Level access is set up by STEER Administrators as required: STEER have a 'School Group' function which brings individual school platforms together under a specific login for STEER school group leads to oversee their schools. These can be configured according to country, region or entire group as needed for any number of staff. Platform UI: The senior team members within a school can each be allocated top school level (Level 5) permissions to view all reports, overviews and pupil assessment data, plus school analytics comparison data as well as the Administration/Tech and IT functions granted to Level 3 IT Leads as below. These credentials are generated on request by STEER Administrators. Pupil Assessment Cohort Data: Level 4 staff access is set by in school Level 5 practitioners using a simple permissions matrix and allows for the configurations of different access arrangements depending on the cohorts a particular member of staff should be able to view. Level 4 staff will have no access to the action plans or cohort reports outside of their permissions granted by Level 5 staff and will not have Technical and IT function access. The platform will automatically send out new Level 4 credentials to staff if their username is set as their email address. IT/Technical: Level 3 permissions are granted by STEER to the IT Leads and will only give access to the administration and technical setup features they require for that role (importing/editing pupil data and exporting logins etc). STEER Administrators are able to alter the permission levels of staff if the correct written authorisation is provided.
11	For what purposes will the personal data be used?
	Pupils-so that the AS Tracking assessments can be run and the AS Tracking assessment data generated Staff-so that granular access can be granted as needed to the assessment data, reports etc
12	Are any of the purposes described above new purposes?
	Yes
13	How will individuals be informed of the purposes for which their personal data is used or do you consider that individuals are already aware that their personal data will be used for the purposes described above? If so, please provide details of how individuals have already been informed.
	Academy privacy notices define the processing purposes of data. Additional comms will be sent to parents/pupils.
14	Who will have the power to change, remove or update personal data?
	The AET Administrators and Data Manager will have full control of the data.
15	Will any portable devices (either personal or issued by AET) be used to store, transfer or access personal data? ***Guidance:*** *This will include laptops, tablets, smartphones, USB sticks, CDs etc.*
	The Teacher mobile App is available to download so that pupil assessment data and action plans can be viewed using the platform credentials. This data is not stored locally but annotations can be added to the action plans which will update the database record. See the USTEER information here: https://steer.global/en/products The AS Tracking Pupil app allows for the assessment to be taken on personal mobile devices or school tablets. The pupils login are the AS Tracking credentials and apart from the assessment data, no additional personal data is captured or stored in the app.
16	Will personal data be disclosed to any third parties (including any group companies) or will any third parties have access to personal data in AET's systems? If so, please provide details, including the purposes for which such third parties will have access to personal data.
	Please see the Staff privacy notice for details of STEER third party processors
17	If third parties will have access to personal data has/will due diligence be carried out on those third parties and what contractual arrangements are/will be put in place?

	Due diligence audits are completed for all third party processors in accordance with the GDPR and recorded in the STEER Data Inventory
18	Please describe the security measures that will be put in place to protect personal data from unauthorised access, loss or damage. Please include details of both technical and organisational measures.
	See the STEER Data Security and Information Governance documents
19	Will any data be transferred outside of the European Economic Area as part of the project or will any person have access to personal data from outside the European Economic Area? ***Guidance:*** *the European Economic Area includes all countries that are members of the European Union plus Norway, Liechtenstein and Iceland.*
	STEER's dedicated Rackspace servers are in the UK (Crawley). See staff privacy policy for details on third party processors support services
20	If an individual makes a request in relation to their personal data (for example a request for a copy of their personal data, a request for data to be deleted or a request to stop marketing), how will such a request be managed and processed?
	Please see the DSA and Staff PP
21	Will any potentially privacy intrusive technologies be used? ***Guidance:*** *This may include, for example, use of facial recognition technology or biometric data such as fingerprints or similar.*
	No
22	How and when will personal data be deleted/ destroyed?
	The data remains under the control of AET at all time, including the assessment data. Please see our data retention policy (Data Security Document)
23	Will the system(s) in which personal data will be stored enable AET to categorise data into datasets that must be deleted and datasets that may be retained? Will the system enable deletion of personal data in a way that prevents reconstitution of the data? Please provide details below.
	Data deletion via the edit pupil record is complete and final for the selected pupil including assessment data. Staff deleted via the edit pupil record will result in the personal data record/credentials (and access to the platform) being deleted/revoked but action plans created on the deleted accounts will remain, but can be deleted separately if required.
24	Will the system(s) in which personal data will be stored enable personal data about a specific individual to be collated into a commonly used electronic format in an automated way?
	No, but there are options to manually download via a CSV the pupil records and separately the assessment results (full) and priority pupil results only Pupil export logins are available to print or download Assessment reports can be exported via email or downloaded in pdf Staff records are not downloadable and the system is blind to staff passwords
25	Will you be carrying out any profiling of individuals using personal data? If so, please provide details of the nature of the profiling, the data that will be used to carry out the profiling and the technology that will be used to carry out the profiling.
	No, AS Tracking is not profiling, it is analysing welfare risks
26	Will the system(s) that hold personal data enable searches to be carried out to locate all personal data relating to a specific individual? Please provide details.
	Individual pupil assessment records are searchable/exportable, as well as pupil logins which can be filtered by form, year etc. There is a search filter in the edit pupil/staff records but no export available for individual pupils/staff

27	Will the system(s) that hold personal data enable data to be corrected and updated?
	Yes, by manual editing and over-writing through import CSV
28	In some circumstances it is necessary to consult with individuals who will be impacted by the project. Have you carried out or do you intend to carry out any consultation with affected individuals? If so, please provide details. If not, please explain why you do not consider that consultation will be necessary.
	NA
29	Are there any other issues that you believe need to be considered or that you are concerned about from a data protection perspective?
	NA

Completed by: -

[redacted]

Section B: Risk Assessment

The purpose of this Section B is to identify privacy and related risks that arise in relation to the project.

This Section B must be completed with input from the Data Protection Officer (DPO) based on the information that is captured in Section A.

In the table below the following terms have the following meanings (if used):

DPA Data Protection Act 2018

GDPR General Data Protection Regulation 679/2016

PEC Regulations Privacy and Electronic Communications (EC Directive) Regulations 2003

	Risk	Mitigation Strategy
1	The proposed anonymisation approach is not robust enough to protect the individuals data	A data sharing agreement will be put into place. The proposal has been assessed from both a data protection and information security perspective.
2	The data used exceeds the requirements of the processing	The data sharing agreement shall stipulate both the data to be used and processing activities. Should the data requirements change a new DSA will be put into place.
3	The assessments produced by the data do not provide an accurate picture of students' current situations resulting in incorrect assumptions being made	AS Tracker shall be used as one of a number of different methods for tracking students' mental health. No judgements about students shall be made on the basis of the assessments alone.

In order to identify the relevant risks, it is helpful to link the issues to the data protection principles and other key requirements of the data protection legislation. Answering the questions in the following table in relation to each principle will help you to identify the risks:

Principle / Requirement	Questions
Fair and lawful processing	
Personal data must be processed lawfully, fairly and in a transparent manner and there must be a legal basis to permit the processing, in particular: (a) at least one of the conditions in Article 6 GDPR must be met, and (b) in the case of special category personal data, at least one of the conditions in Article 9 GDPR must also be met.	● Have you identified the purpose of the project? ● How will individuals be told about the use of their personal data? ● Do you need to create / amend any privacy notices? ● Have you established the legal basis for processing? ● If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
Specified purposes	
Personal data must be obtained only for one or more specified, explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	● Does your project plan cover all of the purposes for processing personal data? ● Have potential new purposes been identified as the scope of the project expands?
● **Adequacy and data minimisation**	
Personal data must be adequate, relevant and limited to what is necessary for the purpose or purposes for which they are processed.	● Is the information you are using of good enough quality for the purposes it is used for? ● Is the data processing proportionate when you balance the objectives of the project against the impact on individuals? ● Which personal data could you not use, without compromising the needs of the project?
● **Accuracy**	
Personal data must be accurate and, where necessary, kept up to date.	● If you are procuring new software does it allow you to amend data when necessary? ● How are you ensuring that personal data obtained from individuals or other organisations is accurate?
● **Data retention periods**	
Personal data processed for any purpose or purposes must not be kept in a form which permits identification of individuals for longer than necessary for that purpose or those purposes.	● What retention periods are suitable for the personal data you will be processing? ● Are you procuring software which will allow you to delete information in line with your retention periods?
● **Individuals' rights**	
Individuals have a number of rights under GDPR which must be respected.	● Will the systems you are putting in place allow you to respond to requests from individuals more easily? ● Can data be rectified or erased if required? ● Can data be extracted in a commonly used electronic format to send to the individual? ● If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?
● **Data security**	
Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	● Do any new systems provide protection against the security risks you have identified? If so, what are they, how are they implemented and how do they work in practice? ● If a third party data processor is involved have you carried out checks on their information security and data protection practices and procedures?

	• What training and instructions are necessary to ensure that staff know how to operate a new system securely?
• **Overseas data transfers**	
Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	• Will the project require you to transfer data outside of the EEA? • If you will be making transfers, how will you ensure that the data is adequately protected?

Section F: Legal basis of processing

The legal basis for the data processing is as follows (please tick as appropriate and provide further details for each legal basis relied upon). Please note that for special categories of personal data it will be necessary to identify both a personal data legal basis and a special categories of personal data legal basis.

Personal Data:	Tick here if this legal basis is relied upon:	Details:
The individual has consented to the processing		
The processing is necessary for performance of a contract with the individual or to take steps at the request of the individual prior to entering into a contract		
The processing is necessary for compliance with a legal obligation		
The processing is necessary to protect the vital interests of the individual		
The processing is necessary in order to carry out a task in the public interest		
The processing is necessary for the purposes of the legitimate interests of AET or a third party and those interests are not overridden by the privacy rights and interests of the individual	X	
Special categories of personal data:	**Tick here if this legal basis is relied upon:**	**Details:**
The individual has given their explicit consent to the processing		
The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law	X	
The processing is necessary to protect the vital interests of the individual or another person where the relevant individual is incapable of giving consent		
The processing relates to sensitive personal data that has been made public by the individual		
The processing is necessary to establish, exercise or defend legal claims or in connection with legal proceedings		
The processing is necessary in the substantial public interest and is permitted under the UK's Data Protection Act 2018		
The processing is necessary for occupational health purposes or for the assessment of the working capacity of an employee		
The processing is necessary for reasons of public interest in the area of public health		
The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and is proportionate and has appropriate safeguards in place to respect individuals' privacy interests		