Data Protection
Impact Assessment Guidance

Arbor has prepared this document to help our customers who decide to complete a Data Protection Impact Assessment (**DPIA**) as part of compliance with their obligations under the UK General Data Protection Regulation (**UK GDPR**). In this document we offer information about personal data processing within the Arbor Management Information System (**MIS**), and some guidance about how to conduct a DPIA. You can use this document as a starting point, or simply use it to supplement your own DPIA format.

| **Important: Arbor cannot provide legal advice, and nothing in this document should be relied upon as legal advice. The information in this document is not a replacement for reviewing guidance issued by the Information Commissioner’s Office or seeking independent legal advice where necessary.**  |
| --- |

Arbor MIS

## Step One: Identify The Need For A DPIA

*[Explain broadly what the project aims to achieve and what type of processing it involves. It may be helpful to refer or link to other documents, such as the project proposal. Summarise why you identified the need for a DPIA.]*

Arbor MIS is used to capture, analyse and take actions on a range of pupil, staff and school-level data. Arbor MIS enables schools, trusts and/or local authorities to meet their statutory obligations regarding maintaining a Pupil Education Record, as well as meeting their other operational obligations and objectives. When providing the Arbor MIS, Arbor acts as the Data Processor on behalf of schools, multi-academy trusts and local authorities (the “**Data Controller**”).

Under Article 35 of the UK GDPR, a controller is required to carry out a Data Protection Impact Assessment where processing is likely to result in a high risk to individuals. While the Data Controller will ultimately determine whether a DPIA is required in a given case, Arbor has prepared this DPIA in recognition of the fact that the Data Controller’s use of Arbor’s MIS is likely to involve the processing of personal data that relates to children on a large scale, and that such information may include special category and other sensitive personal data, such as ethnicity, medical information and court orders. This DPIA, therefore, provides specific information on the processing operations associated with the Arbor MIS.

## Step Two: 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 another way of describing data flows. What types of processing identified as likely high risk are involved?]*

The Data Controller will determine how and why personal data is processed; however, Arbor has provided an overview below of how personal data is likely to be collected and processed in connection with the Data Controller’s use of the MIS.

1. **Collection:** Arbor initially migrates data from the school’s original or incumbent MIS provider, under the Data Controller’s instruction.
2. **Processing operations**: Arbor understands that each Data Controller (i.e. the school / education authority) will undertake the following processes in relation to the personal data in the MIS:
	1. Collecting personal data from the Local Authority, DfE, parents and other professional bodies;
	2. Recording and organising personal data;
	3. Structuring and storing personal data;
	4. Building and producing reports;
	5. Ingesting / uploading personal data;
	6. Deleting personal data.
3. **Storage**: Arbor’s data warehouse and servers are hosted within Amazon web services cloud storage platforms in the UK.
4. **Third parties:** We integrate with several third-party vendors to allow the Data Controller to take actions such as sending emails, sending SMS messages, processing payments and generating PDF a documents. Arbor has appropriate contractual agreements in place with all its third party suppliers regarding the processing of personal data. A list of Arbor’s authorised sub-processors can be found [here](https://support.arbor-education.com/hc/en-us/articles/360013442894-Arbor-s-Data-Protection-Policy-to-comply-with-GDPR#h_01HFVS5X04M5GRASGV5CTXSHTE). The Data Controller can also appoint other third party processors that connect to Arbor’s MIS using an API subject to their agreeing to our API terms.
5. **Deletion:** The MIS allows Data Controllers to set their own retention policy for their data and how long their data should be stored - see here for more details: [Managing data retention for your MIS data](https://support.arbor-education.com/hc/en-us/articles/360005458217-Managing-data-retention-for-your-MIS-data). The data is destroyed when the Data Controller terminates its Contract with Arbor and after they have received a full database backup of their MIS data following termination. We will also delete as otherwise instructed by the Data Controller.

### 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?]*

The personal data processed by Arbor’s MIS consists of school-level, pupil-level and staff-level data provided by the Data Controller. The categories of personal data may include the following:

* **Student / pupil data:** Student name, address, contact details, emergency contact number, gender, date of birth, Admission Number, enrolment status/history, previous schools, nationality, languages, English proficiency, transport, funding and allowances, behaviour, attendance, assessment, exams, exclusions, reports, learning aims, and the information listed under ‘Sensitive data’ below.
* **Staff data (e.g. teachers and teaching assistants):** Name, date of birth, staff code, contact details, languages, absences, contracts, qualifications, CPD, and certain categories of data listed under ‘Sensitive data’ below.
* **Parent/guardian/carer:** Name, contact details and certain categories of data listed under ‘Sensitive data’ below.

Sensitive data\* includes data regarding:

* Gender
* Ethnicity
* Religion
* Special Education Needs
* Medical Conditions and Medical History
* National Health Service Number
* Free School Meal Eligibility
* Child protection notes
* Details on “in care” students
* Court orders relating to parents & guardians
* Identity documents, including nationality, passport, and National Insurance Numbers
* Criminal record checks and other employment checks (for Staff)
* Safeguarding incidents.

\*Some of this sensitive data is also ‘special category data’ under the UK GDPR.

The data will be updated on a continuous basis for all of the Data Controller’s current, future and former students, parents/guardians and staff.

You may want to include an estimate of the number of data subjects whose data will be processed.

### 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?]*

**Nature of relationship with individuals:** Arbor’s relationship is with the schools and other education authorities, i.e. the Data Controller, who collect and process the personal data of their students, parents and staff. As explained in Step One, when a school or other education authority uses Arbor’s MIS product for the processing activities described in this DPIA, Arbor acts as a Data Processor on behalf of the school, academy or local authority. Arbor does not have a direct relationship with the individuals whose personal data is processed by the Arbor MIS.

**Lawful basis for the processing:** The lawful basis for processing the personal data is determined by the Data Controller. As the MIS is used by schools to meet their statutory obligations of maintaining a Pupil Education Record, as well as to fulfil other operational objectives, Arbor understands that there are a variety of legal bases that may cover this processing activity, including statutory requirements to collect data, statutory requirements to analyse data for the purposes of improving education, exercising a statutory duty of care for the students, and carrying out the processing to meet the legitimate interests of the Data Controller or another third party.

**Individuals’ expectations:** The individuals whose personal data is processed would reasonably expect the schools, multi-academy trusts and local authorities to use the data in this way, including by contracting with suppliers (such as Arbor) who specialise in data analysis and operational management tools to improve how schools operate.

### 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?]*

The Data Controller will determine the purpose for which the personal data is processed. Arbor understands that the Data Controller will use the MIS for effective operational management, and to fulfil their statutory obligations relating to the collection and processing of pupil, parent, carer and staff data.

The purpose of Arbor’s processing is to provide a single cloud-based MIS for schools and educational establishments, so that the Data Controller can fulfil the purposes outlined above.

## Step Three: 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?]*

The Data Controller may decide to consult with relevant stakeholders, such as staff and parents.

It is important to note that, while Arbor is a Data Processor, we have continuously consulted with Data Controllers, i.e. the schools, multi-academy trusts and local authorities, throughout the process of implementation of our management information system and analysis tools, to ensure the tools are useful for achieving the operational and legal requirements of the Data Controller.

We have also consulted with security experts from Amazon Web Services and Protection Group International in the architecting of our infrastructure and ensuring our Information Security Management System adheres to ISO 27001 standards.

##

## Step Four: Assess Necessity and Proportionality

### Describe compliance and proportionality measures

*[What is your lawful basis for processing? Does the processing actually achieve your 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 measure do you take to ensure processors comply? How do you safeguard any international transfers?]*

**Lawful basis**: As explained in Step One, Arbor acts as a Data Processor for schools, local authorities and multi-academy trusts, who are the Data Controller. The Data Controller will determine the lawful basis for the processing. The relevant lawful basis(es) the Data Controller will rely upon is likely to include compliance with a legal obligation and legitimate interests.

**Does the processing actually achieve the purpose?** The purpose of the processing is determined by the Data Controller. As explained in Step Two, the Data Controller will use Arbor’s MIS for effective operational management and to meet their statutory and reporting obligations as a school or education authority. The data collection and subsequent processing through the MIS is considered necessary to enable the school or other education authority to fulfil these operational and statutory requirements. It is important to note that the processing activities subject to this DPIA may already take place within each school (e.g. through their prior or incumbent MIS), so the selection of Arbor’s MIS will not fundamentally change how the personal data is processed in this respect.

**Is there another way to achieve the same outcome?**  The Data Controller will ultimately be responsible for determining whether there is another way to achieve the purposes outlined above. Arbor understands that it would not be possible for schools to discharge their organisational management and statutory obligations without the use of a Management Information System such as Arbor’s MIS.

**How will Arbor prevent function creep?**  As Arbor acts as a Data Processor when providing its MIS, it can only process personal data on the instructions of the Data Controller. This means that all of Arbor’s processing will be approved by the Data Controller and Arbor cannot process the personal data for its own purposes.

**How will Arbor ensure data quality and data minimisation?** The data is inputted by the Data Controller, i.e. schools, local authorities and multi-academy trusts, who have a variety of processes to ensure that data subjects regularly check the accuracy of the data. We also have built-in data quality checking tools.

**What information is given to individuals?** Parents, students and staff can see and amend their own data by logging on to their portals. As the Data Controller, it is the schools’ responsibility to communicate with these individuals to explain the reasons for the processing of their data.

**How will Arbor help to support their rights?** Arbor has a strong information security management regime, in order to minimise the risks of breach or misuse of personal data. Arbor has also implemented built-in tools to help with SARs, deletion requests and the management of data retention policies.

**What measures does Arbor take to ensure subprocessors comply?** We perform annual due diligence on the data hosting infrastructure to ensure that they have maintained their ISO 9001, ISO 27001, ISO 27017 and ISO 27018 accreditations. We perform annual due diligence on sub-contractors such as our Email, SMS and Payments providers to ensure they adhere to their obligations under GDPR.

**How does Arbor safeguard any international transfers?**

Apart from existing transfers to Arbor’s group companies, Arbor will not transfer personal data to, or process personal data in, any third country or territory without ensuring that one of the following appropriate safeguards is in place in respect of the transfer:

1. there has been a European Community finding of adequacy pursuant toArticle 45 of the GDPR in respect of the country or territory that the personal data will be transferred to; or
2. the transfer is to the United States to an importing entity that is a certified member of the UK Data Bridge of the EU/US Data Privacy Framework (DPF); or
3. Arbor and the relevant importing entity are party to a contract in relation to the export of personal data incorporating:
	1. standard contractual clauses in the form adopted by the European Commission under Decision (EU) 2021/914 and the UK Addendum issued by the ICO; or
	2. The ICO’s UK International Data Transfer Agreement (IDTA); or
	3. An equivalent data transfer agreement meeting the requirements of UK data protection laws.

## Step Five: Identify and Assess Risks

Arbor has carried out an assessment of the possible risks associated with the processing subject to this DPIA in order to assist the Data Controller meet its obligations under Article 35. As Arbor is a Data Processor, the analysis below is subject to the understanding that the Data Controller should still conduct their own risk assessment of the processing.

| **Describe the source of risk and nature of potential impact on individuals.** *Include associated compliance and corporate risks as necessary.* | **Likelihood of harm** | **Severity of harm** | **Overall risk without mitigations (see Step Six)** |
| --- | --- | --- | --- |
| *[You should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic damage.]* | *[Remote, possible or probable]* | *[Minimal, material or or severe]* | *[Low, medium or high]* |
| **Unauthorized Access to School Management Information System****Risk to individuals**: Potential disclosure of sensitive personal data.**Compliance risk**: Breach of DPA/GDPR; breach of compliance with any relevant government (e.g. DfE) security policies; possible sanctions**Organisation/reputational risk:** Reputational, operational and financial risk – trust in Arbor and educational data research infrastructure is damaged.Breach of DPA/GDPR creates potential risk of fine from the Information Commissioner’s Office (ICO). | Possible | Material | Medium |
| **Intruder Access to Arbor Servers****Risk to individuals**: Potential disclosure of sensitive personal data.**Compliance risk**: Breach of DPA/GDPR; breach of compliance with government (e.g. DfE) security policies; possible sanctions**Organisation/reputational risk:** Reputational, operational and financial risk – trust in Arbor and educational data research infrastructure is damaged.Breach of DPA/GDPR creates potential risk of fine from the ICO. | Remote | Material | Medium |
| **Data may be kept longer than required****Risk to individuals**: Personal data may be processed longer than is necessary and/or longer than the individuals would expect. **Compliance risk**: Would be a breach of DPA/GDPR legislation and potentially a breach of any government (e.g. DfE) security policies and professional standards.**Organisation/reputational risk:** Reputational, operational and financial risk – trust in Arbor and educational data research infrastructure is damaged.Breach of DPA/GDPR creates potential risk of fine from the ICO. | Possible | Minimal | Low |
| **Data may be transferred to countries with inadequate data protection regimes****Risk to individuals**: If appropriate safeguards are not in place, then personal data may not be subject to the same level of protection as under UK data protection laws when it is transferred to the third country. **Compliance risk**: Breach of DPA/GDPR; breach of compliance with government security policies; possible sanctions**Organisation/reputational risk:** Reputational, operational and financial risk – trust in Arbor and educational data research infrastructure is damaged.Breach of DPA/GDPR creates potential risk of fine from the ICO. | Possible | Material | Medium |
| **Inappropriate disclosure of data about children or vulnerable adults creates potential safeguarding breach****Risk to individuals**: Potential safeguarding issues for children or vulnerable adults**Compliance risk**: Breach of DPA/GDPR; breach of compliance with government security policies; possible sanctions**Organisation/reputational risk:** Reputational, operational and financial risk – trust in Arbor and educational data research infrastructure is damaged.Breach of DPA/GDPR creates potential risk of fine from the ICO. | Remote | Severe | High |
| **Third Party App Vendors disclose sensitive personal data****Risk to individuals**: Potential disclosure of sensitive personal data.**Compliance risk**: Breach of DPA/GDPR; breach of compliance with government security policies; possible sanctions**Organisation/reputational risk:** Reputational, operational and financial risk – trust in Arbor and educational data research infrastructure is damaged.Breach of DPA/GDPR creates potential risk of fine from the ICO. | Remote | Material | Medium |

##

## Step Six: Identify Measures to Reduce Risk

*[Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step Five.]*

The table below identifies the measures Arbor has implemented to address the risks identified at Step Five.

| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Evaluation***Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?* |
| --- | --- | --- | --- | --- |
| *[From Step Five]* | *[Possible examples: deciding not to collect certain types of data; reducing the scope of the processing; reducing retention periods; taking additional technological security measures; providing training and guidance to staff; or offering opt outs.]* | *[Eliminated, reduced or accepted]* | *[Low, medium or high]* | *[Yes/no]* |
| Unauthorised Access to School Management Information System | Arbor has built-in a variety of security measures schools can use minimise the risk of this:* Password policy requiring regular password changes and strong passwords
* Two-factor authentication to login
* All data transmissions encrypted
* Automatic log out after period of inactivity
* Role-based access control system with fine-grained and context-sensitive permissions.

A description of the security measures Arbor has implemented to protect the personal data we process can be found [here.](https://support.arbor-education.com/hc/en-us/articles/360013442894-Arbor-s-Data-Protection-Policy-to-comply-with-GDPR#h_01HFVRKD4KAYMW94EM9VWXPP7R) | Reduced | Low | Yes |
| Intruder Access to Arbor Servers | Arbor has implemented a comprehensive Information Security Management System which covers a range of physical, infrastructure and process-related information security measures. Taken in combination, these act to significantly reduce the risk of information security breaches.The operation of our ISMS is audited annually as part of our ISO 27001 certification.Our data centre also has ISO 9001, ISO 27001, ISO 27017, and ISO 27018 accreditation.A description of the security measures Arbor has implemented to protect the personal data we process can be found [here.](https://support.arbor-education.com/hc/en-us/articles/360013442894-Arbor-s-Data-Protection-Policy-to-comply-with-GDPR#h_01HFVRKD4KAYMW94EM9VWXPP7R) | Reduced | Low | Yes |
| Data may be kept longer than required | Arbor has a data retention policy and deletion process in place, in accordance with our legal agreement with Data Controllers.There is a data retention tool built-in to the Arbor app to allow schools to delete records in accordance with their own retention policy. | Reduced | Low | Yes |
| Data may be transferred to countries with inadequate data protection regimes |  Our data centre is located in the UK. We also use a number of named sub-contractors for essential functions such as sending emails, SMS and producing PDFs. These are all located in the EEA, or the United States, and any transfers are carried out on the basis of an adequacy decision, or for the US, the UK Data Bridge of the EU/US Data Privacy Framework (DPF) certification. Critical subcontractors compliance is assessed annually as part of our supplier due diligence.Where Arbor transfers personal data to another third country, we have appropriate safeguards in place, such as the ICO’s IDTA and/or the UK Addendum to the EU SCCs.Only employees of the company, appropriately trained and with valid criminal records checks may process the data for the purposes of providing technical support to schools or maintenance of our infrastructure. | Reduced | Low | Yes |
| Inappropriate disclosure of data about children or vulnerable adults creates safeguarding breach | Schools as the Data Controller are responsible for discharging their statutory duty to only allow access to student records to persons who are suitable to work with children and vulnerable adults.Arbor has put in place a number of safeguards in respect of its employees who may access data about children. Specifically all Arbor employees must pass the following pre-employment checks:* Identity check
* Two references, one personal and one professional
* Criminal records check (“**DBS Check**”)
* Qualifications checks, where relevant to the job

We operate a continuous training programme to ensure all employees have awareness of the safeguarding risks relating to the data we process, and operational measures to reduce those.If Arbor becomes aware of a safeguarding issue involving an employee, employment would be suspended whilst we work with the Local Authority designated officer to resolve the matter and implement their recommendations (if any).Access to all production systems is logged. | Reduced | Low | Yes |
| Third Party App Vendors disclose sensitive personal data | Schools as the Data Controller must agree to permit additional third party app vendors accessing their data. There is a legal duty upon the Data Controller to ensure that any additional Data Processors comply with their obligations under GDPR.The following measures help to minimise the risk when third parties integrate with Arbor’s API:* Integration partners to enter into an API agreement with Arbor governing their use of our API.
* Documentation and support provided to third parties to ensure they build an accurate and appropriate integration.
* Access control within the API to ensure that schools only share the minimum amount of data necessary to third parties.
* Ability for schools to terminate access in respect of any third party instantly.
* Transparent disclosure to the school of which data items each third party has access to.
 | Reduced | Low | Yes |

##

## Step Seven: Sign Off and Record Outcomes

*[To be completed by the Data Controller]*

| **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* |
| Consultation responses reviewed by: |  | *If your decision departs from individuals' views, you must explain your reasons* |
| Comments: |
| This DPIA will be kept under review by: |  |  |
| Last updated:  |  |  |