 **DPIA**

## **Children’s University Online**

# **Submitting controller details**

|  |  |
| --- | --- |
| **Name of controller** | School |
| **Subject** | Children’s University Online |

# **Step 1: Identify the need for a DPIA**

|  |
| --- |
| As part of running the Children’s University programme in our school, we will be using Children’s University’s online platform, ‘Children’s University Online’ (CUO).  Children’s University is about encouraging, tracking and celebrating our pupils’ participation in activities beyond the classroom. This includes both activities that we run in school, as well as activities run by third parties in our school and activities that children take part in at home or in the wider community. This is a national programme and coordinated locally by Children’s University partners. You can find out more at [www.childrensuniversity.co.uk](http://www.childrensuniversity.co.uk)  As part of the programme, our pupils are given a paper ‘Passport to Learning’ within which they can collect stamp codes for their participation in validated activities. They can then input these in their own online account with Children’s University where they can then see additional information, such as the skills they’ve gained and the interests they are building. As a school, we can also report on this information and use it to gain an insight into our own provision. As this involves uploading children’s information in order to create accounts online, a DPIA is best practice. |

# **Step 2: Describe the processing**

|  |
| --- |
| There are two types of accounts that will be set up online – staff accounts and pupil accounts.  Staff accounts will be set up by our local Children’s University Manager. We will collect data from staff and it will be used by the local Children’s University Manager to set up a user account. It will then be stored on Children’s University Online (secure Azure servers that are based in the UK) and can be deleted by staff, the local Children’s University Manager and the national Children’s University Trust.  Once staff accounts are set up, the School is responsible for uploading children’s information to set up user accounts. Children’s University will collect this from the School data management system and it will be used to set up individual user accounts. It will then be stored on Children’s University Online (secure Azure servers that are based in the UK) and can be deleted by staff, the local Children’s University Manager and the national Children’s University Trust.  All of the data uploaded, both for staff and pupils, will be viewable only within the secure log-in of Children’s University Online by the School’s local Children’s University Manager and the Children’s University Trust team.  Children’s University Trust is the charity at the heart of the Children’s University network, and they are responsible for Children’s University Online.  Image result for school mis  Image result for children's university logoImage result for school clipart |

|  |
| --- |
| **Describe the scope of the processing:** |
| The data processed and the intended use of it is as follows:  **Staff**  Staff who will be coordinating this programme in school will be set up with a user account. The data collected as part of this is:   * \*First and second name (in order to identify them) * \*Nickname (in order to identify them to children – e.g. If staff are commonly known to children by an alternative name) * \*Email address (in order to be used as a log in) * Phone number (in order for Children’s University to contact staff if needed)   Only those marked \* are mandatory. This data will be given to our local Children’s University manager and they will create a user-account for staff.  **Pupils**  Once staff accounts are set up, the School can upload the details of the children that we wish to take part in the programme. The data collected as part of this is:   * \*First and second names (this information is needed in order for certificates to be created, schools to be able to monitor children’s progress, and children to log in) * \*Date of birth – this information is needed in order for Children’s University Trust to be able to target age-appropriate activities at participants. * \*Gender – this information is to assist schools in ensuring that Children’s University participation reflects the gender split of the school. This information may also be used in order to target gender-appropriate activities at participants (e.g STEM for Girls programmes) and encourage inclusion for all. * \*School – this information is needed as all children are grouped into schools using Children’s University Online. * Unique Pupil Reference Number (UPN enables us to use this as an identifying field for comparison with other data exports from other platforms – CUO does not collect any special category data such as ethnicity. Should we wish to compare participation in Children’s University with special category data, then UPN makes this possible).   Only those marked \* are mandatory. A note on these:   * Date of birth is required, but should the School wish to further minimise risk, the School are able to use a generic date of birth. * Name, UPN and Date of birth used accurately will enable the School and our pupils to identify themselves accurately on the Department for Education database. This may be useful in future when Children’s University may be able to be aligned with other datasets such as national schemes for recording achievements. |

|  |
| --- |
| **Describe the context of the processing:** |
| All data uploaded to Children’s University is done so as part of our expected duties as a school in regard to personal development beyond the curriculum. Participation in the Children’s University programme has been proven to impact positively on attainment, increase skills development, and provide a positive association with learning. More on the impact of Children’s University can be found at [www.childrensuniversity.co.uk/evidence](http://www.childrensuniversity.co.uk/evidence)  The Children’s University programme is one that the School have signed up to with the interests of our pupils’ wellbeing and character development in mind. This is our responsibility as a school, as evidenced by the inclusion of personal development in the Ofsted framework.  Children’s University Online is a modern system built by Children’s University Trust and their digital partners, The Tech Dept. The technology is contemporary and maintained on a monthly basis and all data is stored in secure Azure servers that are based within the UK.  As part of our School’s involvement in the Children’s University programme, we work locally with XXXXX who run Children’s University in our area. XXXXX license the Children’s University model from Children’s University Trust and pay a membership fee. As part of their membership, they are able to use Children’s University Online with their member schools, of which we are one.  Children’s University is a long-established programme with a great reputation and an ever-increasing evidence base of making a positive impact on the lives of children. Children’s University Trust is a registered charity and so operate not-for-profit and exist solely to work towards their vision of a world where every child has equal opportunity to unlock their full potential through learning beyond the classroom. |

|  |
| --- |
| **Describe the purposes of the processing:** |
| Participation in the Children’s University programme has been proven to impact positively on attainment, increase skills development, and provide a positive association with learning. More on the impact of Children’s University can be found at [www.childrensuniversity.co.uk/evidence](http://www.childrensuniversity.co.uk/evidence) |

# **Step 3: Consultation process**

|  |
| --- |
| The School does not need to consult with parents or children regarding the School’s involvement with Children’s University as this is an expected part of the School provision.  The School do not need to, or plan to, consult information security experts, but can contact Children’s University Trust at any time regarding any queries relating to security. |

# **Step 4: Assess necessity and proportionality**

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** |
| Under the General Data Protection Regulation the lawful basis used for processing data is one or more of the following:   * Public task (in the case of LA maintained schools) Article 6(1)(e) * Legitimate interest (in the case of independent Trusts) Article 6(1)(f) * Performance of a Contract Article 6(1)(b)   The School should ensure that they have selected and documented the appropriate legal bases for their purposes  Children’s University run a passport scheme that is paper based that would involve not using the online platform, Children’s University Online. However, in not using this system we would not be able to report on availability and participation data and would gain no insight into skills development, interests, and employer engagement. These additional data insights come not from our pupil data, but rather they are the additional data tags with which activities on the platform are tagged with.  The Data shared is the minimum required to provide a straightforward, highly effective education service.  Children’s University are committed to providing all reasonable and timely assistance (including by appropriate technical and organisational measures) to the School to enable the School to respond to:   * Any request from a Data Subject to exercise their rights under Data Protection Law (including their right of access, correction, objection, erasure and data portability, as applicable and subject to any exemptions) * Any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the processing of the Data. |

# **Step 5: Identify and assess risks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| 1. **Source of Risk** - Inaccurate data provisioned. Risks would include non-compliance (data being accurate and up to date) as well as corporate risks (loss of credibility, risks of enforcement action, press coverage etc). **Article 5(1)(d)**   **Potential impact** on individuals would include loss of confidentiality and potential embarrassment depending on nature of inaccurate data processed. The School is responsible for the accuracy of the data.  **Mitigation** – The School must ensure that the data shared is accurate and up to date.   1. **Source of Risk** - Platform processing more personal data than is required for the purpose. **Article 5(1)(c)**   **Potential Impact** on individuals would include loss of confidentiality, potential embarrassment and potential harm depending on the nature of the data processed.  **Mitigation** – only the minimum amount of data is shared to achieve the purpose.   1. **Source of Risk –** Sharing of personal data to unauthorised third parties. Risk would include non-compliance (data not used for specified and explicit and legitimate purpose) and corporate (loss of credibility, enforcement action being taken, press coverage, possible legal actionfor personal compensation etc) **Article 5 (1)(f)**   **Potential Impact** on individuals would include loss of confidentiality, potential embarrassment and even harm depending on the nature of the data transferred incorrectly.  **Mitigation** – Terms and Conditions clearly defined in the Data Processing Agreement specifying sub processors and third-party processors.   1. **Source of Risk** – School staff email addresses unprotected personal data to the platform. This can occur when there is a need for support whereby school staff see issues with the data and email the personal data to support staff for investigation. **Article 5(1)(f)**   **Potential Impact** on individuals include their data being seen by data processor’s staff, the dangers inherent in emails being sent to incorrect recipients, loss of confidentiality, possible embarrassment or harm depending on the nature of the exposed data and its final recipient.  **Mitigation** – CU support School staff but do not require password information.   1. **Source of Risk** – Personal data kept longer than necessary. The School as the data controller must ensure that data is deleted when a pupil leaves the School or transfers to a new school in order for the download from the School MIS to CU to comply with **Art 5(1)(e)**   **Potential Impact** on individuals include their data being inaccurate which may result in loss of confidentiality and breach of Data Subjects rights.  **Mitigation –** Regular downloads to be undertaken to ensure records remain accurate and up to date and those no longer required are securely deleted. | Remote, possible or probable  Possible  Possible  Remote  Probable | Minimal, significant or severe  Significant  Minimal  Significant  Minimal | Low, medium or high  Medium  Low  Low  Low |

# **Step 6: Identify measures to reduce risk**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| Inaccurate Data – breach of Article 5.1(d) | The School must ensure that the data provided to the data processor is accurate and up to date | Eliminated reduced accepted  Accepted | Low medium high  Medium | Yes/no  Yes |

# Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/position/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 |
| DPO advice provided: |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice:  Given that the data parameters contain personally identifiable information there is always a risk when sharing information with a third-party. However, robust policies and procedures are in place to help prevent any loss or unauthorised access to the data. The School must ensure that the data is kept accurate and up-to-date and delete data when no longer relevant or required. | | |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |