

Title: Virtual Events Privacy Impact Assessment

Date: 26 June 2020

Version: V1.0

Status: Final

Security Marking: Internal Use Only

Privacy Impact Assessment Template

This template is to record the Privacy Impact Assessment (PIA) process and results where personal data is being processed in a new manner. Details should be completed from the beginning of the project; step one of this form will identify if a full PIA is required due to the potential high-risk nature of the processing activity.

PIAs are used to help us identify the most effective way to comply with our data protection obligations and meet our customers' expectations of privacy. They are designed to identify 'privacy risks' or data protection concerns at an early stage and reduce associated costs and damage to reputation caused by non-compliance. This guidance follows the standards set out by the Information Commissioner's Office (ICO) together with the [Article 29 working group](#) and applies to personal data relating to customers and employees.

Information privacy risks relate to the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent or reasonable expectations, misuse of information, as well as through surveillance and monitoring.

The General Data Protection Regulations (GDPR) and accompanying Data Protection Act 2018 (DPA) requires the completion of Data Privacy Impact Assessments, as defined in Article 35 of the Regulations, when there may be high risk to the rights and freedoms of the individuals whose personal data we process. Within UCAS Data Privacy Impact Assessments will be known as Privacy Impact Assessments for continuity purposes.

Under GDPR, all completed full PIAs must be sent to the Information Governance Manager, via datagovernance@ucas.ac.uk, in their role as Data Protection Officer to be reviewed and approved. If a PIA has risks that cannot be eradicated, but are significant, then the Information Governance Manager will have to consider further discussion at the Data Governance Board, with the Senior Information Risk Owner (SIRO), or it may require review by the Information Commissioner's Office (ICO) as part of the 'prior consultation' process. This can take a significant period of time, so early engagement with Information Governance is encouraged. Ultimately the ICO has the power to require organisations to cease intended or actual processing activity if it considers the activity to be an unpalatably high risk.

Step One – Initial screening questions

Screening questions	Enter Y/N
Scale: Will the project involve the collection of <u>new</u> information about individuals on a large scale?	N
Innovative Technology: Does the project involve using new technology which might be perceived as being privacy intrusive or is a novel application of existing technologies (including Artificial Intelligence)?	Y – initial attempts are virtual events and therefore a potential high risk processing activity when reviewing the number of individuals/ types of stakeholders involved in
Significant effect: Are you making decisions about an individual's access to services based on automated decision?	N
Large-scale profiling: Are you intending to use the data for large scale profiling of individuals?	N
Biometrics: Are you intending to process biometric information i.e. fingerprint IDs or facial recognition?	N
Data matching: Are you intending to use the personal data for data matching purposes e.g. combining, comparing or matching personal data obtained from multiple sources?	N
Invisible Processing: Are you carrying out invisible processing e.g. where the information has been obtained from third parties and not the data subject and where we have not notified the data subjects of that processing?	N
Tracking: Are you tracking or monitoring data subjects e.g. geolocation, behaviour, online activity etc.?	N
Targeting of children: Are you processing personal data to target children or vulnerable adults for marketing purposes, profiling or other automated decisions, or offering online services to children?	Y – provision of an events booking service intended for individuals researching their future journey to Higher Education. Registrants for events will in the majority be under the age of 18, but the service is not available to anyone under the age of 13.
Risk of physical harm: Are you processing personal data which, if compromised by a data breach, it could jeopardise the health and safety of the individuals?	Y – Yes, there is a potential risk that exposure of data from a virtual event could expose individuals to

	harm from identify theft or unsolicited contact.
--	--

If you answered yes to any of the above, please go the Step 2 and engage at this stage with the Information Governance Team.

If you answered No to all questions, you do not need to complete a PIA. If you are not sure you can contact the Information Governance team at datagovernance@ucas.ac.uk for advice.

Step Two – Provide a background to the project and consultation

1. Explain what the project aims to achieve, what the benefits will be to UCAS, to our customers and any other relevant party.
2. Draw on what was identified within the initial screening questions to summarise why the need for a PIA was identified.
3. If helpful, please link to other relevant documents related to the project, for example a project proposal.

The provision of a programme of Virtual Events is an initially tactical solution to the Covid-19 control measures and impact on UCAS' events offer. This initial provision also provides an initial foothold in the virtual events market going forward for exhibitors and visitors.

The PIA is required as this incorporates the use of new technology to provide a service to UCAS customers following a successful initial proof of concept event. The virtual events offer will be accessed by users under 18 primarily, and therefore in accordance with ICO guidance is seen as a higher risk form of processing.

Consultation requirements

In order to ensure that UCAS identifies all privacy risks, consider who might need to be consulted, both internally and externally. This should be linked to all relevant stages of the project and can be done at any stage.

A proof of concept event was provided in June 2020 to allow for the review of Ivent together with preparing the groundwork for a full roll-out. The event involved a range of interested parties including registrants, parents, advisors and exhibitors. Feedback from the event was provided and used to review the value of the offer to participants across the board and develop the rollout of a wider virtual event process.

Wider consultation on the virtual events offer has included a student webinar and direct feedback from advisors in advance of setting up the proof of concept event.

Step Three – Describe the information flows

The collection, use and deletion of personal data should be described here. It may be useful to do this in the form of a flow diagram and link it into this document. This section should provide brief details of what data is collected and why, where it will be held and how it is managed and the categories of data subjects (i.e. learners, advisors, representatives, UCAS or provider staff etc.).

Please include the potential number of individuals that are likely to be affected in the above flow.

Personal data will be obtained direct from pre-applicants, parents, advisors and exhibitors as part of the relevant registration processes. Registration is completed on a UCAS.com page incorporating the requirements of the Ivent registration process.

Data collected reflects information currently collected to support physical events including:

Exhibitors:

First name *
Last name *
Organisation name*
Email address *
Mobile number

Advisors:

First name *
Last name *
Position/Job title*
Email address *
Mobile number
School/college name*
Address *
School type

Parents:

First name *
Last name *
Email address *
Mobile number
Address *
Which subjects is your son/daughter interested in studying at a higher level? *
When would he/she like to start university? *
Is he/she interested in studying an apprenticeship*

Student:

First name *
Last name *
Email address *
Mobile number
DOB*
School/college name*
Address *

Which subjects are you interested in studying at a higher level?*

When would you like to start university?*

Are you interested in studying an apprenticeship*

With all attendees' interactions with stands, including the use of chat functionality to ask questions about the course provision etc. will be retained and accessible. As the offer is reviewed in terms of the provision of 1 to 1 video chat this PIA will be expanded further as per the initial risk identified within this PIA document.

Pilot and strategic architect designs available at:



Wider integrations may not be available in full with the tactical 2020/21 solution; but learning from these events will assist requirement gathering for future developments/ procurement activity in this area.

Step 3: Data Protection Compliance

1. Types of data subjects

Type of data subjects			
Learners	X	Referees	
UCAS Employees	X	Agents	
Providers	X	Advisors	X
Suppliers		Other (Please note)	Data subjects will include parents wishing to support their child with their decision making.

2. Special category data

Confirm if any special category data is processed			
Religion or beliefs		Genetic data	
Race or ethnic origin		Health	
Political opinions		Sex life	
Trade Union Membership		Criminal convictions	

No special category data is explicitly collected through the virtual events system. The running of a virtual event provided a reduction in the requirement to process special category data as there is no requirement to request details of physical impediments which may cause attendance difficulties and reasonable adjustment requirements within a physical event.

3. Lawful basis for processing (You may wish to review the content on "Lawful basis for processing" in our [Privacy Policy](#))

Data protection law requires us to have a lawful basis for processing personal and special category data. The list below refers to the relevant provisions in the General Data Protection Regulations. State Yes for the ones that apply to this form of processing.					
Personal Data – Article 6			Special Category Data – Article 9		
6(1)(a)	Consent	x	9(2)(a)	Explicit consent	
6(1)(b)	Performance of a contract	x	9(2)(b)	Employment, social security, social protection law	
6(1)(c)	Legal obligations		9(2)(c)	Vital interests	
6(1)(d)	Vital interests		9(2)(d)	Not-for-profit body	
6(1)(e)	Public interest / Official Authority		9(2)(e)	Made public	
6(1)(f)	Legitimate interests		9(2)(f)	Legal claims / Judicial	
Data Protection Act 2018 Schedule 1: <i>[Add here if relevant]</i>			9(2)(g)	Public Interest	
			9(2)(h)	Medicine, employee capacity, medical diagnosis, health or social care	
			9(2)(i)	Public health	
			9(2)(j)	Archiving, scientific and historical research or statistical purposes	

Legal basis is split into three parts under this process:

Personal data of registrants (including pre-applicants, parents, advisors and representatives of exhibitors) are processed under contract in the supply of access to a virtual event in terms of attendance or representation at an event.

Consent provides the legal basis for UCAS derived marketing activity through the issuing of opt-in options to receive education updates or commercial offers. Such consents are provided to a registrant dependent on status (pre-applicants) and then join the mailings journey managed by the Insights Team within operations. As the Virtual Events programme is offered through the use of an external supplier's infrastructure the mastering of consents within SAP CDC is not currently possible and static consents will be obtained and managed by UCAS. Individuals will be provided within the normal opportunities to opt out of mailing within communications as required.

Consent also provides the legal basis for the provision of contact information to exhibitors once a stand has been visited by a delegate (dependent on status). This mirrors the approach currently used for physical events; however, there is an additional step of a delegate scanning their barcode to confirm the consent to share their data. This additional process is not possible within this current process. This consenting for data to be shared with exhibitors is noted within information surfaced to event attendees together with further confirmation within the UCAS Privacy Policy which is presented to individuals when they sign up to an event.

4. Consent

Key areas	Questions	Response
Consent	If you rely on consent to process the data for this activity (i.e. marketing), please confirm consent is an affirmative action, you have recorded when it was given and have a process to log when it has been refused or withdrawn. Where feasible, consent preferences should be recorded and managed through UCAS' Enterprise Preference Management Solution.	<p>Consent is used as a legal basis for onward marketing by UCAS as per the current opt-in journey. It is additionally used as a legal basis to share contact information to exhibitors where an individual has visited and exhibitor's virtual stand.</p> <p>UCAS marketing consents will be managed through the current marketing journeys and individuals are able to unsubscribe at any point via links in the messaging or contacting UCAS direct. In terms of exhibitor consents these are provided as a single snap-shot of consent available to exhibitors to provide further information to an individual and as the exhibitor will be data controller for this information, once shared, they will need to ensure relevant</p>

		<p>unsubscribe provisions and further details are provided in accordance with Data Protection law requirements.</p> <p>Please see the notes with the legal basis text above for further information on the surfacing of consents.</p>
--	--	---

5. Source of the personal data and transparency

Key areas	Questions	Response
Source of the data	Confirm where you are getting the personal data from for this activity. Are you using existing data, collecting it from the data subjects, or from a third party?	Personal data processed through the virtual events platform will be sourced directly from data subjects.
Notification	If you are collecting new data directly from the data subjects, have you got a privacy notice in place to tell them what you are doing with their data?	A link to the UCAS privacy policy to provided as part of the registration process and includes specific content about the handling of virtual events data.
	If you are collecting from a third party, are you intending to contact the data subjects to let them know the processing is taking place?	N/A

6. Data protection principles

Key areas	Questions	Response
Limited purpose	When you collect or obtain the personal data for this activity, do you intend to use it for any other purpose?	<p>Data is processed to support the provision of a virtual events offer including access to content exposed during individual events. Data is also used to provide marketing opportunities on a consent basis, together with the provision of contact details to exhibitors visited by an individual during an event.</p> <p>Data may also be used to produce anonymised statistical outputs and/or research into progression to higher education in accordance with the provision of data protection law and appropriate business or public interest reporting.</p>

Data minimisation	<p>When you collect or obtain the personal data for this activity, are you being selective and processing the minimum necessary?</p> <p>Can the personal data be anonymised or pseudonymised?</p>	<p>Only minimum data is requested to support the facilitation of the event attendance and offer.</p> <p>Personal data is required to ensure that individuals can appropriately engage with the event and exhibitors. Details provided also ensure tailored information and advice can be provided.</p>
Accuracy	Are you confident the personal data you process is accurate and do you have a process in place to check the quality and improve data quality errors or inconsistencies?	<p>As data is provided directly by data subjects any data accuracy concerns should be limited.</p> <p>Validation should be undertaken if any anomalies take place during the extraction of event data to ensure accuracy.</p>
Storage limitation (retention)	Do you have retention schedules in place that state how long this personal data will be held for?	Retention periods are detailed in the UCAS retention policy and data will be managed in accordance with these requirements.
Retention and disposal	Is the personal data destroyed in line with the agreed retention rules are there reasons why it cannot be destroyed e.g. resources, IT constraints, etc?	Contractual requirements are in place for the return and secure destruction of data by the events platform supplier at the end of the contract. Data held by UCAS include data outputs and consents can be managed and destroyed in accordance with the retention schedule and records management policy.
Integrity and confidentiality	Is the personal data protected, so that it cannot be altered or changed by any unauthorised personnel whilst in storage or transit?	Data hosted in AWS instance and encrypted. Secure https: encrypted connection used on registration website during data collection for each event. Secure site also provides data extraction facilities for UCAS and exhibitors with back-end/ exhibitor access respectively.

7. Data subject rights

Key areas	Questions	Response
Access to personal data	Do you have a procedure to handle subject access requests?	Yes – see Subject Access Request Process available from the Information Governance intranet page.

Guidance	Are data subjects provided with guidance about how to request access to the personal data held about them?	Yes – Guidance is available on the UCAS website via the privacy policy
Location and retrieval	Can the personal data held about a data subject be identified, retrieved and provided to the data subject within the one month deadline? Either manually or through a self-service process.	Yes, data can be manually extracted from the Ivent system and relevant downloads to handle SARs as required.
Data portability	Can data subjects get their personal data in a structured, commonly used and machine-readable format?	This is unlikely to affect UCAS as there is no current specific alternative applications provider; but, may be relevant if the proposal relates to alternative processing of information.
Erasure and notification	Are individuals informed of their right to erasure or rectification of personal information held about them (where applicable)?	Yes – Guidance is available on the UCAS website via the privacy policy
	Are there controls and formal procedures in place to allow personal data to be erased or blocked?	Yes – see Retention Policy and approach to Right to be Forgotten available from the Information Governance intranet page.
Right to object	Are individuals told about their right to object to certain types of processing?	Yes – Guidance is available on the UCAS website via the privacy policy
Profiling and automated processing	Is any of the personal data used for data matching or profiling? <i>If it is likely that solely automated decision-making may cause a legal effect on individuals, without human intervention, then this must be raised with the Information Governance Team immediately</i>	N/A – no such processing will be undertaken through this service.

8. Data security

Key areas	Questions	Response
Secure transmission of personal data	Is the personal data secure when being collected e.g. online forms, portals, recordings, etc. Should this require encryption in transit?	Data hosted in AWS instance and encrypted. Secure https: encrypted connection used on registration website during data collection for each event. Secure site also provides data extraction facilities for UCAS and exhibitors with back-end/ exhibitor access respectively.

Secure storage of personal data	Is the personal data secure when in storage (encryption at rest)? If yes, provide details if possible?	As noted above the AWS instance is encrypted as rest to ensure data integrity.
Overseas Data Storage	Is the data sent or stored overseas outside of the European Economic Area (EEA) i.e. cloud storage?	AWS is hosted in EU data centre (Ireland)
User access controls	Are access controls and user rights in place to prevent unauthorised access, and are they reviewed and kept up to date, including administrator access?	Events Technical Team will manage UCAS colleagues access to events and related data.
User Training	Have the people authorised to process the personal data completed data protection training e.g. UCAS induction or bespoke systems-based training with a data protection element?	Training of all staff re: DPA and information security occurs during induction and subsequent refresher training and awareness activity. UCAS use of the system will be managed by the Events Technical Team with support provided as required.
	Are the staff and other authorised users using IT systems, given training before they access the live system, or do they train in the live system e.g. work shadowing?	UCAS use of the system will be managed by the Events Technical Team with support provided as required.
Use of live data for system testing	Is personal data needed for system testing or can dummy data be used? If live data is needed can it be anonymised? If live data is required, has this been signed off by Enterprise Security and Information Governance colleagues?	Live data testing not required for this project.
Business continuity	Can the personal data be restored in a timely manner in the event of a technical or physical incident?	Ivent use AWS infrastructure to host data with core backup facilities. UCAS downloads will be backed up as per standard internal IT infrastructure provision.

9. Data sharing and 3rd party processing

Key areas	Questions	Response
Data Processors	Is the personal data held given to third parties to process on our behalf, e.g. contractors? If so, do we have a contract / data processing agreement to cover all the expected responsibilities?	The virtual events programme is supported by the data processor Ivent who provide the technology to facilitate virtual events. This processing is governed by a contract directly with the supplier which has been specifically reviewed for data protection compliance.

Sharing personal data with third parties	If information is part of regular information sharing with a third party organisation i.e. HESA, is an Information Sharing Agreement in place?	An exhibitor will receive a copy of the contact details of attendees that visit their stand under the terms of their exhibitor terms and conditions. Once data is shared they take data controller responsibility and must handle that information in accordance with data protection law
--	--	---

Step Four – Identify privacy and other related risks

Use the table below to identify the key privacy risks and any associated compliance and corporate risks. If any larger risks are identified, then consideration needs to be given to whether they should be recorded on the corporate risk register as related compliance risks.

Due to the significantly high penalties for the loss, misuse, damage and inappropriate disclosure of personal data, we must identify and mitigate the risks identified within this document wherever possible.

The common risks are the loss, theft or physical damage of personal data; unauthorised access, alteration or deletion of personal data; the breach of confidentiality of personal data. These risks can have potential consequences for the individuals concerned, as well as UCAS, and our partners or contractors, potentially causing physical harm, distress or embarrassment to individuals and resulting in reputational damage, loss of public trust, extensive financial penalties or legal action.

Use the table below to list the privacy risks associated with this processing of personal data, the solutions to treat the risk and the decision. The 'Mitigation activity/ Project requirements' column must state the risk control and decision actions may include efforts to Accept, Reduce, Remove or Transfer the risk in accordance with the UCAS risk management process.

The most common risks have been listed in the table below as a guide, but you will need to add your own risks, or expand on or delete those listed, according to your own project.

If you have any queries about the privacy risks, contact the Information Governance Team datagovernance@ucas.ac.uk.


Risks and controls

Risk No.	Privacy Risk/ Impact	DP issue	Mitigation activity/ Project requirements	Action Owner	Risk Decision	Date
1	Personal data is processed unfairly and / or unlawfully due to lack of transparency	Fair and lawful	Review and publish privacy notices that comply with data protection law and covers this form of processing - e.g. what data, why processed, who its shared with, etc. Privacy policy updated to include reference and processing of virtual events during POC		Mitigated	25/06/2020
2		Fair, lawful and transparent	Secondary use of personal data e.g. data matching, migration – including live, anonymised, pseudonymised personal data – is made clear to the data subjects via the privacy notice. Use of data for analytical/ research purposes covered in privacy policy. Marketing provision separately noted in within PN and within information provided to individuals during registration journey		Mitigated	25/06/2020
3		Specified purposes	Procedures are in place to ensure personal data is processed in accordance to the privacy notice. Guides to exhibitors on use of exhibition data. These will be reviewed on Information Governance before the initial event is launched		Reduce	Review prior to 23 rd July
4		Lawfulness	Where consent is needed to process all or part of the personal data, the consent, its refusal or withdrawal, must be recorded along with the date taken.		Mitigate:	25/06/2020

			Opt out to commercial comms provided within marketing communications and unsubscribe list management			
5	Personal data is unlawfully destroyed, lost, altered, or disclosed due to insufficient electronic security countermeasures in the transfer or storage of that data.	Security	A security assessment has been made of the of Ivent and security requirements identified within the associated contract		Reduced	25/06/2020
6		Security	Data is hosted with the EEA, in this case Ireland reducing risk or non-UK DPA or GDPR compliance issues.		Removed	25/06/2020
7		Security	Data is suitably encrypted during end to end use including during transfer and at rest in storage systems. Confirmation provided within security checklist review.		Reduced	25/06/2020
8	Personal data is unavailable because of electronic or physical access to the information repository	Lawfulness	Procurement and contract discussions confirm the viability of suppliers and data processors in terms of system resilience and recovery. Requirements detailed within contract and associate service level requirements.		Reduced	25/06/2020
9		Adequate and relevant	Back up, disaster recovery and business continuity plans are in place to recover information or regain access as quickly as possible. Ivent data hosted with supported AWS environment and UCAS extractions mitigated by UCAS recovery and backup plans.		Reduced	25/06/2020

10	Personal data is altered accidentally or intentionally altered or deleted	Security	Access controls and user privileges are in place to restrict access to personal data on a need to know basis. Access for UCAS staff will be limited to relevant roles requiring access to registrant details.		Reduced	25/06/2020
11		Security	Access controls and user privileges are reviewed regularly and changed or revoked as necessary. Primary backend access will be managed by the Events Technical Team and review access regularly.		Reduced	25/06/2020
12		Security	One of the most impactful risks to any data held in an organisation is a breach of data protection requirements by employees themselves in terms of human error, bad practice or malicious intent against the organisation. This risk is mitigated by a number of the controls noted in this assessment including access controls, monitoring, training, performance reviews and having clear guidance to staff on the handling of personal data. This risk will always be present but mitigation activities including the reactive review of data security breaches will look to foster a data protection compliant environment within UCAS and its employees.		Reduced	26/06/2020
13	Personal data is disclosed inappropriately to a third party	Security	Training, awareness and guidance is available to help staff understand their data sharing responsibilities, supported by the Information Governance Team		Reduced	26/06/2020

14		Security	<p>Personal data is sent securely to external third parties i.e. secure email encryption, recorded delivery, etc.</p> <p>Exhibitors will have access to the secure details of their exhibition data to review and securely download interactions with their stand. Events and Analysis Teams will securely share data using Moveit or encrypted email if third party disclosure is required outside of the system.</p>		Reduced	26/06/2020
15	Personal data held is accurate and, where necessary, kept up to date	Accurate and up to date	<p>Procedures are in place to manage changes to core personal data held in systems, like name, address and contact details, etc., to prevent information being sent to the wrong person or address.</p> <p>Registrations are provided on a per event basis ensuring that up to date personal data is used in a timely fashion and entered directly by data subjects reducing the risk of data quality issues.</p>		Mitigated	26/06/2020
16	Personal data is kept for longer than necessary	Adequate, relevant and limited	<p>Record keeping procedures make it clear to staff what personal data is needed and where it needs to be held, e.g. In applications, Network Drives, Outlook, SharePoint, physical file, etc.</p> <p>Virtual events records will be retained in accordance with the UCAS retention schedule.</p>		Reduce	26/06/2020
17		Retention	<p>There is a facility to delete records either on a come to notice basis (request to be forgotten) or on a staged basis in accordance with the retention requirements.</p>		Reduce	26/06/2020

			IG to review and action such requests with support of Events Team. Any unsubscribe requests to UCAS' marketing activity can be completed by through normal processes			
18	Video chat functionality, heightened level of privacy intrusion	Privacy and safeguarding	<p>The one to one live video chat function is not being used with the initial event provision in July. This functionality is seen as an enhanced provision for UCAS in the virtual events offer, but does highlight potential privacy and safeguarding concerns.</p> <p>As a result a review is currently underway to consider the impact and mitigation in the provision of this service specifically in reference to the annotation of any outstanding risks and technical or other controls available to mitigate the risk</p>		Risk review in progress	26/06/2020

Step five – Sign off and record the PIA outcome

Who has approved the ongoing privacy risks involved in the project?

Data Protection Officer (DPO)

Summary of DPO advice: The movement to a virtual events provision provides a more technically focused form of processing that our standard physical events. The data governance and security checklist has been reviewed by both Information Governance and Enterprise Security to ensure that the new supplier provides an adequate level of protection with the data obtained, hosted and shared through their system. As this is a new venture use of, and any weaknesses in the systems or related processes should be monitored and reported to our Team where appropriate to review the impact on data privacy.

Step six – Integrate the PIA outcomes into the project plan

Who is responsible for integrating the PIA outcomes into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Contact points for future privacy concerns and role:	This PIA will be kept under review by:
<div>Events Systems and Support Manager</div>	<div>to support developments as they are introduced such as 1:1 video.</div>

	<i>The DPO will also review (where appropriate) ongoing compliance with the PIA and Data Protection legislation</i>
--	---