Title: Privacy Impact Assessment for Clearing Plus

Date: 25 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 new information about individuals on a large scale?	Potentially, Clearing Plus is a new method for servicing the previous Direct Contact Service (DCS) due to the previous service being primarily signed up to upon initial registration take-up of Clearing Plus may be higher. The free to provider offer in the initial year of provision is likely to see a reasonably wide take up by providers hoping to showcase their courses and attract targeted individuals.
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)?	N/A – algorithms are used to link individuals to specific courses/ HEPs but there is no decision making or specific action against an individual and their data through this process. Although options are displayed in a algorithm derived pattern in an attempt to display courses in terms of relevancy, individuals retain choice around selecting course providers to share their details with.
Significant effect: Are you making decisions about an individual's access to services based on automated decision?	No, as noted above potential course choices are surfaced to individuals but they make an active decision if they wish to engage with the relevant provider.
Large-scale profiling: Are you intending to use the data for large scale profiling of individuals?	Although aggregated applicant behaviour and

	previous decision making by applicants is used to support the development of the Clearing Plus algorithm as noted above the options of courses provided to applicants within clearing does not meet the definition of profiling which would cause 'significant effect'. Individuals retain choice over which courses to indicate interest and request more information.
Biometrics: Are you intending to process biometric information i.e. fingerprint IDs or facial recognition?	No
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?	No
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?	No
Tracking: Are you tracking or monitoring data subjects e.g. geolocation, behaviour, online activity etc.?	No
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?	Yes, extended online service to children 17-18
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?	Yes, there is a potential risk that exposure of data from Clearing Plus or the wider UCAS application service 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.

Clearing Plus is a new product that UCAS is looking to offer to Providers and applicants for Clearing 2020. Providers will be able to choose which courses, entry and acceptance criteria they want to feed into a matching algorithm. The matching algorithm will show relevant and available courses to unplaced applicants from early July. The unplaced applicants will be able to view the matched courses via a secure portal, that they can access via Track. Applicants will then indicate whether they want to express an interest in a course or not, with their details being passed on to the course provider if they choose to express an interest. Providers will then be able to review the information provided through Clearing Plus and weblink to identify if they wish to contact the applicant with further details of course options or to discuss an offer. Individuals will then be able to make an offer and the applicant can add it as a Clearing choice.

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.

The majority of research with applicant/ student groups has been done via the Learner Focus Group, last time this was a topic was back in November 2019 when the group discussed clearing plus as a replacement for DCS: Courteney outlined some of the proposals for the DCS replacement - the majority were bought into with the ideas and felt that they would help reduce some stress, in an already stressful time. They clearly found the additional information and help being offered would be of benefit to those in a difficult situation.

Additional webinars and communications have been completed with HEPS to engage them with the process. This engagement activity has continued during testing and initial rollout to providers for course submissions. Feedback received has been used to develop the initial release of the product

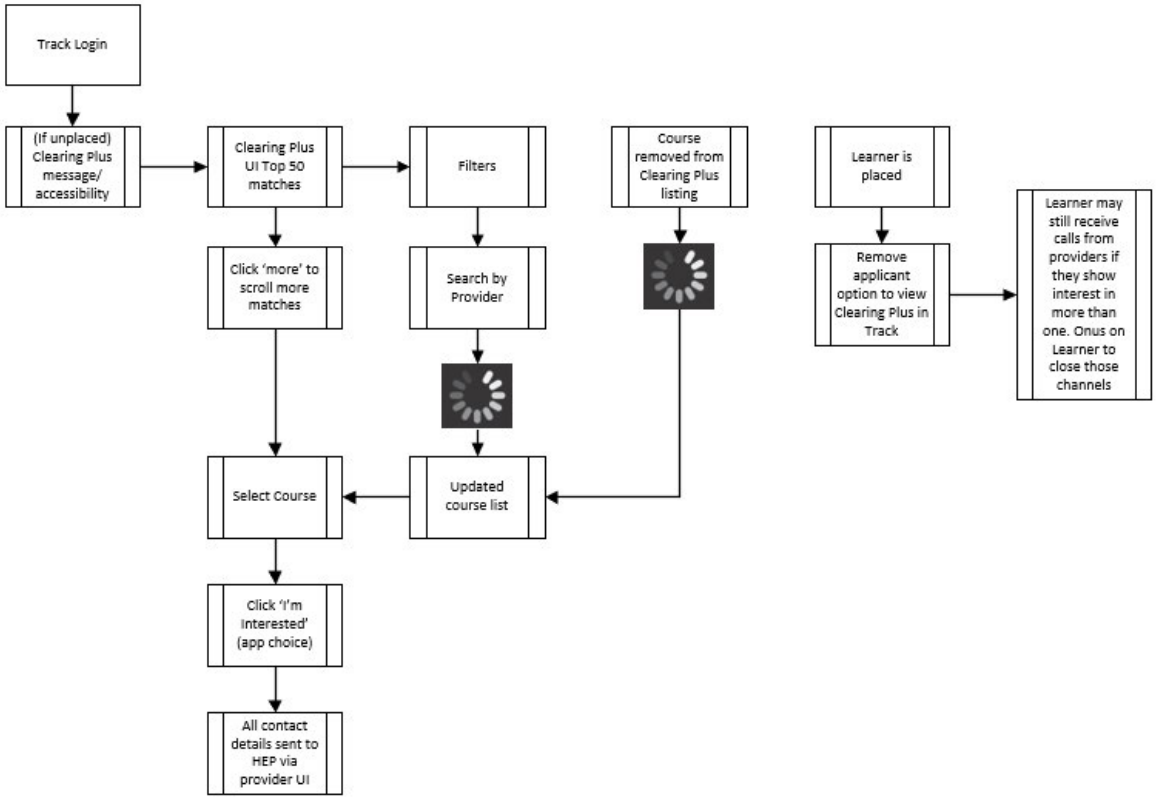
and develop an initial roadmap for future developments. Two Learner webinars have been held to support development and consideration of the product the latest held on the 23rd June.

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.

Data flow documentation for Clearing Plus (MVP view)



The latest Clearing Plus architectural design can be view here: Clearing Plus Architectural Design

Minimum valuable learner journey (including provider and UCAS requirements)
Clearing Plus available to unplaced applicants and learners going direct to clearing (including international) from Clearing opening until closure (not during embargo). Available before & after results with predicted grades and post SQA/A Level results with actual grades. Learner can opt-in

easily and information will explain expression of implications in terms of receiving communications from providers on the selected or similar course options which may be suitable.

Learner sees list of courses with an option to select their interest in a course and receive additional information. A&I algorithm produces results and User Interface displays. Courses they see have been selected by providers as available in Clearing *and* match criteria set as people they are looking for.

When learner clicks 'Interested' course / provider details available using link (Search). Learner details passed to provider. Interested course stays in list distinguished from others. List refreshes when courses availability changes. Learner adds clearing choices in Track once received offer and once they accept the place, they will no longer have access to or visibility of Clearing Plus as they will no longer be unplaced.

Step 3: Data Protection Compliance

1. Types of data subjects

Type of data subjects			
Learners	✓	Referees	
UCAS Employees		Agents	
Providers		Advisors	
Suppliers		Other (Please note)	

2. Special category data

Confirm is 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 will be processed specifically under the Clearing Plus service.

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		9(2)(a)	Explicit consent	
6(1)(b)	Performance of a contract	✓	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: ***[Add here if relevant]***			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	

Processing will be an extension of the current applications management contract to extend to the provision of the Clearing Plus service selected by applicants to whom the service is available and wish to use it.

4. Consent

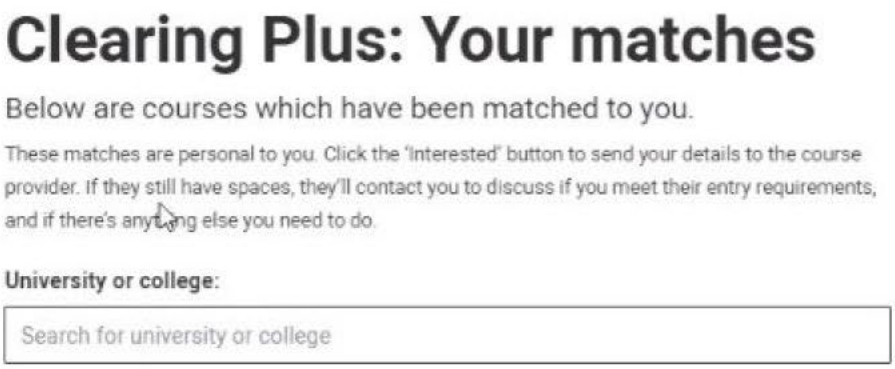
Key areas	Questions	Response
Consent	If you rely on consent to process the data for this activity (i.e. marketing), please confirm consent is an affirmative action, you have recorded when it was given and have a process to log when it has been refused or withdrawn. Where feasible, consent preferences should be recorded and managed through UCAS' Enterprise Preference Management Solution.	N/A

5. Source of the personal data and transparency

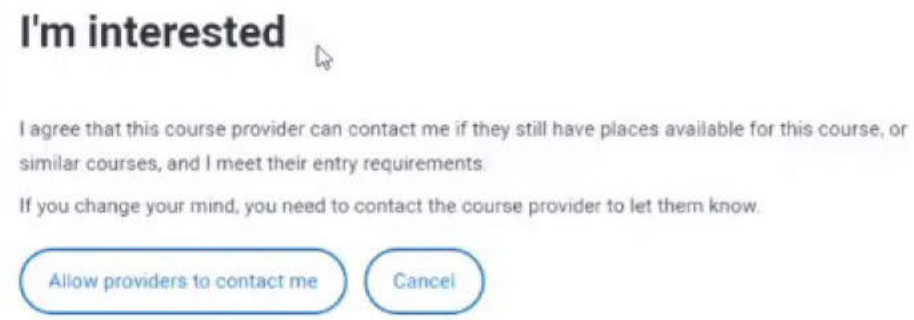
Key areas	Questions	Response
Source of the data	Confirm where you are getting the personal data from for this activity. Are you using existing data, collecting it from the data subjects, or from a third party?	Learner generated content is the primary source of data within Clearing Plus. Data processed is that provided by the learner during the application process or later updated via Track. Third party data matching would occur in terms of in cycle qualifications submissions provided and matched through current ABL processes. The new personal data obtained though this product is the confirmation of the decision to use Clearing Plus and the courses/providers they decide to share their 'interested' marker with.
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?	Limited new personal data will be collected as noted above. The user will be made aware of the service, it benefits and how data will be exchanged with providers if they wish to use the service and select providers to contact them re: specific courses. See the screen prints at the end of this section. Further information in relation to the use and data processing under Clearing Plus will also be included in the UCAS privacy policy.

	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

Prompt for applicants when they enter Clearing Plus:



Details provided when an applicant selects the "I'm interested" button beside a course option and prior to their data being shared with the provider on first selection. This is not shown multiple time to support customer experience.



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?	Data will be used solely for the provision of the Clearing Plus service and the production of related metrics at service wide levels.
Data minimisation	When you collect or obtain the personal data for this activity, are you being selective and processing the minimum necessary?	No addition data captured above the course options which are the output and functionality of the service and any interested in clicks identified by individuals.

	Can the personal data be anonymised or pseudonymised?	
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?	N/A data is user generated, including the contact data which will be shared with the providers applications decide to share their data with.
Storage limitation (retention)	Do you have retention schedules in place that state how long this personal data will be held for?	Preference information will be held only while Clearing Plus is live (to end of Cycle) as no further onward business value or legal basis for retention. This will be deleted from AWS at end of cycle and only anonymised statistical outputs may be retained via the Data Warehouse.
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?	See above – data deleted after cycle. The intention is to provide a data lake output of choice/ use of service anonymised for analytical purposes and therefore no specific data protection concerns.
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?	The service will be available via our secure https site providing encryption in transit. The service has been penetration tested and the associated report highlighted good coding practice and limited vulnerabilities.

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.	Drawing back of data will be possible to identify Clearing Plus use during the application cycle. Details of matches retained during cycle to provide to a requestor if requested. Alternatively they will be able to self-serve their preference

		information through the Clearing Plus function via Track/Apply.
Data portability	Can data subjects get their personal data in a structured, commonly used and machine-readable format?	Data can be provided in a machine-readable format if required through systems outputs. This is unlikely to be a right exercised in respect to the Clearing Plus service.
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? *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*	The data held on applicants will be matched with the Clearing Plus algorithm to expose potentially relevant courses from providers signed up to the service based on the criteria they have set. No specific decision-making or related privacy risk will be exposed by this processing as the decision to engage with the service and share data with providers will be self-selected by applicants.

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?	Where an individual selects to share data with selected providers this will be shared via private secure APIs.
Secure storage of personal data	Is the personal data secure when in storage (encryption at rest)? If yes, provide details if possible?	Data produced within Clearing Plus will be held in AWS and encrypted at rest as standard.
Overseas Data Storage	Is the data sent or stored overseas outside of the European Economic Area (EEA) i.e. cloud storage?	Data will be hosted within AWS within the EEA.
User access controls	Are access controls and user rights in place to prevent unauthorised access,	Access controls will reflect the Apply service internally and HEP transmitted contact data for

	and are they reviewed and kept up to date, including administrator access?	applicants will be supplied under current secure routes and access controls.
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 has been provided to CXC staff to support the management of any enquiries from applicants. Access will be surfaced through Track with CXC able to view matching selection.
	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?	Training has been provided to relevant staff (primarily CXC) in advance of system go live to support enquiry management.
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?	Dummy data will be used for testing in accordance with normal C&C data testing. Data testing was specifically reviewed by Information Governance and Enterprise Security to ensure appropriately anonymised data was used in testing stages for the product.
Business continuity	Can the personal data be restored in a timely manner in the event of a technical or physical incident?	Continuity plans are in place for Track. Storage of preference information and returned choices will be held in a separate bucket in AWS and covered by current cloud continuity protections.

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?	No third party processing occurs through Clearing Plus, with the exception of hosting of identified courses and related choices within AWS, which is managed under our current contract.
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?	Contact information will be shared with the applicant selected providers surfaced within the system. Applicants will make an affirmative action to share their personal information to stimulate contact from a provider via the 'I'm interested' option. Providers will only be able to see and download a list of

		personal contact details and related course to support contact with the individuals. Full application details will only be surfaced directly once a clearing choice has been submitted by the applicant with the relevant provider. Providers can use weblink products to review additional information based on the applicants PID before they confirm a place through clearing.

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 dataxxxxxxxxxx@xxxx.xx.xx.

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. Requirement to update privacy policy to indicate the Clearing Plus process and remove the reference to the previous DCS. To be amended in advance of go live. Suggested text shared with Clearing Plus Team for review.		Mitigate PENDING	Pending
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. Suggested text shared with Clearing Plus Team for review.		Mitigate PENDING	Pending
3		Specified purposes	Procedures are in place to ensure personal data is processed in accordance to the privacy notice. Personal data held as a result of an applicant using Clearing Plus will only be retained during the relevant application cycle and only anonymised statistics retained. This data will not be used in another way.		Remove	11/02/20
4	Personal data is unlawfully destroyed, lost, altered, or disclosed due to insufficient electronic security	Security	Clearing Plus will be access via the secure https contention in Track and the new AWS infrastructure has been PEN tested before public launch.		Reduce	25/06/2020

	countermeasures in the transfer or storage of that data.					
5		Security	Data is hosted with the EEA or within a third country with an adequacy rating or other third-party relevant accreditation. Clearing Plus data will be held with AWS within the EEA		Remove	11/02/20
6		Security	Data is suitably encrypted during end to end use including during transfer and at rest in storage systems via Track and AWS where dated is encrypted		Reduce	11/02/20
7	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 to Track is limited to relevant UCAS employees and onward access to Clearing Plus outputs by HEPs will be managed by providers themselves.		Reduce	11/02/20
8		Security	Access controls and user privileges are reviewed regularly and changed or revoked as necessary. UCAS access to track will be limited to UCAS employees and access removed in accordance with the SLAM process. HEPs are responsible for the management of access to link products and identified within the terms of service.		Remove	11/02/20
9	Recovery of data	Adequate and relevant	Personal data is backed up within current AWS requirements and contract. Admissions service can be run if the Clearing Plus functionality was lost reverting to standard clearing process.		Reduce	11/02/20
10		Security	One of the most impactful risks to any data held in an organisation is a breach of data protection requirements by employees		Reduce	11/02/20

			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.			
11	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. This includes current guidance to CXC staff to ensure that application enquiries are only discussed with an identification checked applicate or their nominated representatives.		Reduce	11/02/20
12		Security	Personal data is sent securely to external third parties. In the case of Clearing Plus data will be shared with providers via private secure APIs/ link products.		Reduce	11/02/20
13	Personal data held is accurate and, where necessary, kept up to date	Accurate and up to date	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. All Clearing Plus data will be applicant driven and applicants will be able to		Reduce	11/02/20

			update contact information either through Apply or via CXC where changes are required.			
14	Personal data is kept for longer than necessary	Adequate, relevant and limited	Record keeping procedures make it clear to staff what personal data is needed and where it needs to be held. In the case of Clearing Plus individual level data should not be removed from the system except by exception. Personal information will only be retained during the relevant cycle and then removed.	[redacted]	Reduce	11/02/20 Deletions required at end of cycle.
15		Retention	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. The risk of right to be forgotten requests is considered low as data is only retained during the relevant admissions cycle. Data can be removed from source systems if required.	[redacted]	Reduce	11/02/20
16	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
17	Removal of "I'm interested option"	Lawful basis/ Accurate and up to date	Under the MVP release of Clearing Plus for the 2020 cycle Clearing Plus users will not be able to remove their "I'm interested" option in real-time. As noted above individuals are advised to contact a provider if they no longer wish to be contacted. Due to the csv	[redacted]	Reduce	25/06/2020

			download provided to HEPS and likely differing approaches to the management of enquires between HEPs UCAS cannot control the contact between the HEP and the individual. The 'consent' to share via the interested in option is a snapshot and HEPs must take into consideration the wishes of the applicant when communicating with them. I.e. once they are placed with another provider or no longer wish to pursue a place at their institution.			

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: During the MVP release of Clearing Plus all data sharing activity and preference collection will be based on an applicant deciding to use the service. This includes data sharing with HEPs which the applicant has decided they wish to engage providing only contact details initially. Wider application data will only be released once a clearing choice has been selected as per the current application process, or where a provider searches an applicant via their PID using link products. There are limited risks to the handling and collection of personal data through this process, the main issue is ensuring that appropriate transparency information is provided to applicants during their signing up to the service and the requirement to ensure the additional process is secure as per the PEN test arranged by Enterprise Security.

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:

(Lead Project Manager) (Product Owner)	(Lead Project Manager) (Product Owner) *The DPO will also review (where appropriate) ongoing compliance with the PIA and Data Protection legislation*