Data Protection Impact Assessment Procedure

1. Introduction

1.1. In order to deliver our mission to provide outstanding residential adult and community education the College collects, uses and stores personal data about a range of individuals including staff, suppliers, students, governors, parents and visitors.

1.2. The College takes the protection of all personal data extremely seriously.

1.3. The College's approach to data protection is set out in its Data Protection Policy. The completion of a data protection impact assessment for any proposed new or revised process, product or service which involves personal data which is likely to result in a high risk to the rights and freedoms of individuals forms part of this approach.

2. What is a DPIA and when should it be used?

2.1. The data protection impact assessment (DPIA) procedure is designed to enable the College to systematically and thoroughly analyse how a particular project, system or business process could adversely impact on an individual's right to the protection of their personal data. The assessment will be used to explore the risks to data protection that could arise, set out appropriate controls and solutions that could be implemented to mitigate or eliminate the risks and ultimately be used to decide whether a project should go ahead.

2.2. A DPIA should be conducted for any **new project, system or business process** (or where **changes are proposed to existing systems or business processes)** which involves the collection and/or processing of personal data and is likely to result in a high risk to the rights and freedoms of individuals. *For the ease of reference this document uses the term 'project' to cover any relevant activity.*

2.3. Examples of the type of project could include:

- a new IT system for storing, processing and accessing personal data;
- a data sharing initiative where two or more organisations seek to share or link sets of personal data;
- a proposal to identify people in a particular group or demographic and initiate a course of action;
- using existing data for a new and unexpected or more intrusive purpose;
- a new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV);
- a new database which consolidates information held by separate parts of the College;
- legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.

2.4. Where appropriate a DPIA should be completed as early as possible in the development of, or change to, any relevant project as this is likely to enable it to have the most positive impact.

3. What is the purpose of a DPIA?

3.1. The purpose of a DPIA is to ensure that privacy risks to individuals are minimised, whilst allowing the aims of the College to be met whenever possible.

3.2. Undertaking robust DPIAs where appropriate will enable the College to:

- clearly establish the purpose and justification for the collection and processing of any personal data;
- comply with its data protection responsibilities;
- protect the personal data of staff, students, visitors and any other relevant individuals;
- provide reassurance to its staff, students, stakeholders and visitors that it is managing and using personal data responsibly;
- build trust with the people using its services;
- increase transparency and make it easier for individuals to understand how and why their information is being used;
- identify potential problems early and implement less costly solutions;
- minimise the amount of information being collected or used where possible, and devise more straightforward processes for staff;
- increase the awareness of privacy and data protection issues within the College and ensure that all relevant staff involved in designing projects think about privacy at the early stages of all their projects.

4. Do I need to undertake a DPIA?

4.1. The College should consider undertaking a DPIA for any project involving the use of personal data.

4.2. A DPIA <u>must</u> be undertaken for any project that is **likely to result in a high risk** to individuals, including any project which will:

4.2.1. use systematic and extensive profiling or automated decision-making to make significant decisions about people;

4.2.2. undertake profiling on a large scale;

4.2.3. use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit;

4.2.4. include the processing of special-category data or criminal-offence data on a large scale;

4.2.5. systematically monitor a publicly accessible place on a large scale;

4.2.6. use particularly innovative technology or organisational solutions;

4.2.7. collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’);

4.2.8. combine, compare or match data from multiple sources;

4.2.9. track the location or behaviour of individuals;

4.2.10. process personal data that could result in a risk of physical harm in the event of a security breach;

4.2.11. profile children or target marketing or online services at them.

4.3. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. An assessment about whether a DPIA is required should therefore be made for all projects involving the use of personal data.

4.4. If it is decided that a DPIA is not required the reasons should be documented.

5. Support Available

5.1. You must consult with the Data Protection Officer regarding any new or revised project involving the use of personal data about whether a DPIA is required.

5.2. Support to complete a DPIA is also available from the Data Protection Officer and/or your manager.

5.3. Guidance is also available from the ICO at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

6. What happens once the DPIA has been completed?

6.1. Once your DPIA is completed it must be:

- reviewed by the Data Protection Officer, who will suggest any amendments or additions and provide any advice;
- considered by the Leadership Team, along with any comments from the Data Protection Officer.

6.2. The Leadership Team will be asked to approve the project based on whether appropriate use of personal data has been demonstrated and whether reasonable controls are planned to eliminate/mitigate any potential risks.

6.3. This may include further action being stipulated to enable the project to proceed.

6.4. In the extremely unlikely event that a high risk is identified which cannot be mitigated and the College still wishes to continue with the project the ICO must be consulted before any processing can commence.

Data Protection Impact Assessment

Project Name	
Project Manager	

Step One – Do I need to undertake a DPIA		
Explain broadly what the project aims to achieve and the type of processing and personal data it involves.		
Will your project:	**Yes**	**No**
Use systematic and extensive profiling or automated decision-making to make significant decisions about people?	□	□
Include carrying out profiling on a large scale?	□	□
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	□	□
Include the processing of special-category data or criminal-offence data on a large scale?	□	□
Systematically monitor a publicly accessible place on a large scale?	□	□
Use any particularly innovative technological or organisational solutions?	□	□
Combine, compare or match data from multiple sources?	□	□
Process personal data in a way that involves tracking individuals' online or offline location or behaviour?	□	□
Process personal data that could result in a risk of physical harm in the event of a security breach?	□	□
Include processing data concerning vulnerable data subjects?	□	□
Process biometric or genetic data?	□	□
Process personal data without providing a privacy notice directly to the individual?	□	□
Include profiling children or targeting marketing or online services at them?	□	□
Process personal data that could result in a risk of physical harm in the event of a security breach?	□	□
Involve collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	□	□
Include tracking the location or behaviour of individuals?	□	□

Decision		
Is a DPIA required?	Yes □	Please continue to step two.
	No □	Please outline your reasons below and forward this form to the data protection officer.

Why is a DPIA not required?

Name	
Date	

Describe your project

What does your project aim to achieve?

Does your project involve:	Yes	No
Using personal data already held by the College for a different purpose	□	□
Collecting new information not currently processed by the College	□	□
Significantly amending a current procedure/system to process personal data	□	□
Introducing a new procedure/system to process personal data	□	□
Other, please outline below:	□	□

What benefits will there be for the individual, College, others?

Why is a DPIA required?

Describe the processing to be undertaken

How will you collect, use, store and delete the data?

Where will you get the data from?

Will you share the data with any individuals or organisations outside the College? If yes, who, how and why?

Will any third party be involved in processing the data, if yes who and why?

Describe the personal data involved

Whose data will be involved?	Student	□	Visitor	□
	Employee	□	Other	□
			Please describe	
What data will be involved? e.g. name, contact details, course work				

Will any special category data be involved?	Health Data □ Trade Union Membership □ Political Opinions □ Religion □ Racial or Ethnic Origin □ Genetic Data □ Biometric Data □ Sex Life/Sexual Orientation □
Will any criminal offence data be involved?	Yes □ No □
How many individuals' data will be involved?	
Will any children's data be involved?	Yes □ No □
Will any data from vulnerable individuals be involved?	Yes □ No □
How often will the data be collected?	
How long will the data be retained? What will be the process for data destruction? How will the data be disposed of?	
Who will access the data? Why? How? When?	

What is the context for the data processing?

Describe the nature of the relationship with the individuals involved, how much control will they have over their data and would they expect us to process it in this way? Are there any 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 should be factored in?

Compliance and Proportionality

What will be the legal basis for processing the data?	Contract □ Public Task □ Legal Obligation □ Legitimate Interests □ Vital Interest □ Consent □
What will be the legal basis for processing any special category/sensitive data?	

How will we inform the individuals involved about the data processing?	
If the legal basis for processing is consent how will this be collected and managed?	
Describe why the processing is necessary, could the objective be achieved in another way?	
Will the data be used for automated decision making/profiling?	Yes □ No □ If yes please describe:
Will any data processing be undertaken by a 3rd party?	Yes □ No □ If yes who, what protocols and safeguards will be in place?
How will the data be stored and where? What security features will be in place?	
Who is the data shared with? Why? Where are they? How is it shared? What protocols and safeguards will be in place?	
Will any data be transferred to a country outside the European Economic Area?	Yes □ No □ If yes, which country, describe the measures in place to mitigate risks and ensure adequate security measures.

Consultation Process

Describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve in the College? Do you need to consult a processor? Do you plan to consult information security experts, or any other experts?

What are the key privacy risks and proposed solutions?

Risk Describe the source of the risk and nature of the potential impact on individuals, include corporate and compliance risks as necessary		Prob-ability	Impact	Score	Measures to reduce or eliminate risk	Effect on risk Eliminated, reduced or accepted	Residual Risk Low, medium, high	Measure Approved Yes/No
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
		High	5					
		Medium	3					
		Low	1					

Project Approval
Summary – Data Protection Officer Advice
Leadership Team Comments

Outcome

Project approved	□
Further action required before project can be approved	□
Unmitigated risks identified – consultation with ICO required	□
Project not approved	□

Comments

Signed		Date	
Name			

Glossary

personal data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
data processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
profiling	any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
consent	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Sensitive/special category data	personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
legal grounds for processing the data	(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). (d) Vital interests: the processing is necessary to protect someone's life. (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)