Data Protection Impact Assessment Procedure

1. Introduction

1.1. In order to deliver its mission to provide outstanding adult residential and community education the college needs to collect, use and store personal data about a range of individuals including its staff, suppliers, students, governors, parents and visitors.

1.2. The college takes the protection of all personal data it collects and processes 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 new or revised project which involves the collection and/or processing of personal data 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** which involves the collection and/or use of the personal data of individuals, or where **changes are proposed to existing systems or business processes**. *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 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 our 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. If your project includes the collection and/or processing of personal data then you will need to complete a DPIA. See glossary for definition of personal data.

4.2. Answer the following questions, if you answer yes to any of them please complete a DPIA:

- Will the project involve the collection of new data about individuals?
- Will personal data about individuals be disclosed to organisations or people who have not previously had access to the data?
- Are you using personal data about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the data about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

5. Support Available

5.1. Support to decide whether you need to undertake a DPIA and/or to complete one is available from the college data protection officer (Sarah Johnson).

5.2. Additional advice is 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 will be:

- reviewed by the data protection officer, who will suggest any amendments or additions;
- forwarded to the leadership team for consideration, along with 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.

Step One – About the Project
Describe your project What need is the project addressing? What benefits will there be to the college, to individuals or to others? What is the purpose of collecting the data? Are there any alternative approaches that could be taken? Why are they not being considered?
Step two: About the Personal Data
Describe the personal data your project will collect/process What personal data will you be collecting and/or processing?
Will any of the data be sensitive (special category) data (see glossary for definition)?
What will the legal grounds for processing the data be (see glossary for definition)?
Who will the data subjects be, how will they be informed of the purpose of collecting the data and if relevant their right to access, rectify, delete, restrict processing, portability and object?
How will the data be collected? Who will provide the data and when?
Will the data be reviewed/updated? When? How?
How will the data be used and why?
Who will access the data? Why? How? When?
Will the data be used for automated decision making/profiling?
Will any data processing be undertaken by a 3rd party? 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 the data leave EU borders?
How long will the data be retained? What will be the process for data destruction? How will the data be disposed of?
Step Three Consultation requirements
Explain what consultation activity you will undertake? How will you carry out the consultation? Who with?

Step Four - What are the key privacy risks and proposed solutions?				
	Risk	Proposed Controls/Solutions	Are the controls in place already? ✓	Result: is the risk eliminated, reduced, or accepted?
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Step five: Project Approval

Data Protection Officer Comments

Leadership Team Comments

Project Approved

Signed		Date	

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 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.)