2.11.4	**Data Protection Impact Assessment ('DPIA')**
	From the previous section it has been determined that the personal data you are collecting requires a Data Protection Impact Assessment ('DPIA').
	'Data protection by design' means embedding data privacy features and data privacy-enhancing technologies directly into the design of a project at an early stage. This will help to ensure increased protection for individual data privacy throughout the lifecycle of a research project. A key component of data protection by design is the DPIA.
	The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation.
	The DPIA also provides evidence that the risks to individuals have been considered and sufficient measures have been taken to protect those individuals.
	The DPIA assesses the activity to be carried out against all the principles of data protection and determine whether the processing of personal data is both necessary and proportionate or whether changes to the process or additional controls are required.
	What is a DPIA and why may it be required / beneficial for a Research Project?
	A DPIA is a process designed to identify risks arising from of the processing of personal data and to manage these risks from as early as possible during the lifecycle of the project. It also demonstrates compliance with the GDPR.
	It is a mechanism for assessing the impact of new initiatives or new technologies and implementing measures to minimise or reduce associated risks.
	DPIA completion is frequently required as a key component of research project design.
	A DPIA is particularly important in instances where the research utilises new technologies or, taking into account the nature, scope, context and type of processing, **is likely to result in a high risk to the rights and freedoms of individuals**.
	The DPIA process and outcomes will help to improve the design of a research project and enhance communication about data protection risks with relevant stakeholders such as research partners, third parties and participants.
	Please review the <u>Questions</u> and associated <u>Guidance</u> in the section below carefully.

	Question	Help Text	Guidance
2.11.4.11	*I confirm that all accounts created on relevant software systems have passwords configured which comply with the Trinity Password Policy: i.e. Minimum of 8 characters, mixture of upper lowercase and special characters.*	It is a requirement that the answer to this question is 'Yes'.	Username and passwords are utilised at Trinity to facilitate access to Trinity IT resources. They also protect Trinity data from access by unauthorised individuals both internally and externally. The College Information Systems Security Policy and supporting policies, including Password Policy, available at: https://www.tcd.ie/ITSecurity/policies/supporting-policies.php.