2.11.5	**Processing Risks**		
	Question	**Help Text**	**Guidance**
2.11.5.1	*List the processing risks of any kind.*	For each of the risks listed the following three questions will be generated.	Different projects carry different risks, and these should be considered. The list below are examples and are intended as a guide, not an exhaustive list. Describe the source of risk and nature of potential impact on individuals. Include associated Compliance and Corporate risks as necessary. Examples of applicable privacy risks are listed below, and the risks associated with the project should be included. **Risks to individuals - examples** • Hacking of computers where project data is stored. • The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. • Incorrect or overuse of individuals' data. • Lack of transparency, fairness or lawfulness of processing activities. • Failure to explain effectively how data would be used. • New surveillance methods may be an unjustified intrusion on their privacy. • Measures taken against individuals as a result of collecting information about them might be seen as intrusive. • The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect. • Identifiers might be collected and linked which prevent people from using a service anonymously. • Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. • Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. • Anonymisation techniques chosen may turn out to be ineffective. • Use of technology capable of making visual or audio recording may be unacceptably intrusive. • Information which is collected and stored unnecessarily or is not properly managed so that

			duplicate records are created, presents a greater security risk. • If a retention period is not established information might be used for longer than necessary. • Lack of effective governance. **Compliance risks** • Non-compliance with the common law duty of confidentiality. • Non-compliance with the Data Protection Acts 1988-2018/ General Data Protection Regulation (GDPR), Privacy and Electronic Communications Regulations (PECR). **Associated organisation/corporate risks** • Non-compliance with the data protection or other legislation can lead to sanctions, fines and reputational damage. • Problems which are only identified after the study has commenced are more likely to require expensive fixes. • The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with Trinity College. • Public distrust about how information is used can damage Trinity's reputation and lead to loss of business. Data losses which damage individuals could lead to claims for compensation.
	Question	**Help Text**	**Guidance**
2.11.5.2	*Solutions/mitigation actions.*	Indicate the actions being taken to reduce or eliminate each of the identified risks.	Each risk identified must have a Risk Likelihood, Risk Severity and Risk Score. The identified risk should include solutions/mitigating actions and whether they have been implemented. After the actions have been taken, please indicate what the residual/remaining risks will be – is the risk Unchanged, Reduced or Eliminated. Please state what the new risk score is, after the mitigating actions are taken.