GDPR & DATA PROTECTION ACT 2018 – ADDITIONAL CHECKLIST (9)
DATA PROTECTION IMPACT ASSESSMENTS

DPIA awareness checklist

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

☐ Our existing policies, processes and procedures include references to DPIA requirements.

☐ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.

☐ We have created and documented a DPIA process.

☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

☐ We always carry out a DPIA if we plan to:

☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people.

☐ Process special category data or criminal offence data on a large scale.

☐ Systematically monitor a publicly accessible place on a large scale.

☐ Use new technologies.

☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.

☐ Carry out profiling on a large scale.

☐ Process biometric or genetic data.

☐ Combine, compare or match data from multiple sources.

☐ Process personal data without providing a privacy notice directly to the individual.

☐ Process personal data in a way which involves tracking individuals' online or offline location or behaviour.

☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.

☐ Process personal data which could result in a risk of physical harm in the event of a security breach.

☐ We consider whether to do a DPIA if we plan to carry out any other:

☐ Evaluation or scoring.

☐ Automated decision-making with significant effects.

☐ Systematic processing of sensitive data or data of a highly personal nature.

☐ Processing on a large scale.

☐ Processing of data concerning vulnerable data subjects.

☐ Innovative technological or organisational solutions.

☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ If we decide not to carry out a DPIA, we document our reasons.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

DPIA process checklist

☐ We describe the nature, scope, context and purposes of the processing.

☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our data protection officer.

☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.

☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ We identify measures we can put in place to eliminate or reduce high risks.

☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ We implement the measures we identified, and integrate them into our project plan.

☐ We consult the ICO before processing, if we cannot mitigate high risks.

☐ We keep our DPIAs under review and revisit them when necessary.