

**Adopted : Summer 2023**

**Review : Summer 2024**

 **Signed…………………………………………………............(Chair of Trust Board)**







**Data Protection**

**Impact Assessment**

**Guidance to the Data Protection Impact Assessment Template**

The GDPR requires controllers to carry out data protection impact assessments (DPIAs) when:

* using new technologies; and
* when processing is likely to result in high risk to the rights and freedoms of individuals.

Processing that is likely to result in high risk includes (but is not limited to):

* Systematic and extensive processing activities, including profiling where decisions have legal effects – or similar significant effects – on individuals.
* Large scale processing of special categories of data (all data known as sensitive personal data under the Data Protection Act 1998 plus genetic and biometric data) or personal data relating to criminal convictions or offences.
* Large scale systematic monitoring of public areas (e.g. CCTV).

Further guidance is expected on what constitutes high risk processing.

Where your DPIA indicates that your planned processing would be of high risk in the absence of risk-mitigating measures taken by the controller, the controller is required to consult the supervisory authority (the ICO) prior to proceeding.

Therefore when looking at your processing activities (what you are doing with any personal data that you hold), if you are doing anything that may put the individuals at risk – either because there is a risk that their data may be revealed or disclosed, or there is a risk of an invasion into privacy (such as with CCTV systems), then you need to carry out a DPIA.

**Data Protection Impact Assessment template**

**This form sets out 7 questions you need to ask yourself before you start or continue the risky processing activity.**

1. What is it that you want to do with the data?

*(Here, you need to identify what it is you want to do, in as much detail as you can. Describe what information is collected or used, what it is used for, who it is obtained from and disclosed to, who will have access to it and how many people are affected. As an example, if you are installing CCTV, can you say how many cameras and where? Which data subjects will be affected? What use will be made, and by whom? What are the views of the general public on this type of operation?)*

1. What are the benefits of what you are doing?

*(Why are you considering the action identified above? What benefits will it bring to you? What are you likely to gain from it? Why do you consider it necessary? There must be a legitimate interest being pursued in a necessary and proportionate way.*

1. What are the risks to the rights and freedoms of data subjects?

*(What is the likely impact on individuals if you implement the course identified above? What risks exist to the individual? What is the likely impact on the individual’s general right to privacy? Have you consulted, internally and externally, to identify and address privacy risks?)*

1. What steps can you take to mitigate the risks identified above?

*(Having identified the risks, is there anything that you can do to mitigate those risks? List everything that you could do – even if it is something that you will not end up implementing. Identify how the action mitigates the risk, and whether you would consider it a possibility, having regard to the purpose of what you are considering doing. Include any future steps that may be necessary – for example future security testing. Do you need to amend your privacy notices?) Cover safeguards, security measures and mechanisms to ensure the protection of personal data.*

1. Should we consult with data subjects before taking this step?

*(Who are the relevant data subjects? Can they participate in the consultation effectively? What process will you use to take account of any views expressed?)*

1. Do the benefits outweigh the risks, taking into account any mitigation that you will put in place?

*(This is the final conclusion – set out whether the benefits outweigh the risks first, and your reasons for reaching this conclusion. Relevant to this will be an analysis of the potential steps you could take to mitigate, and identify which of those you will implement, and why. The mitigated impact on individuals must be necessary and proportionate to the aim you set out to achieve.)*

1. How will the DPIA be given effect?

*(How are the mitigation steps and other measures under the DPIA to be built into the project and who will be responsible for ensuring they are carried through? The controller should review implementation if there is a change in risk as a result of the processing.)*