APPENDIX 2

Draft/DATA PROTECTION IMPACT ASSESSMENT POLICY

Data Protection Impact Assessments (DPIAs) help Hertsmere Borough Council (the Council) identify, assess and mitigate or minimise privacy risks with data processing activities. They are particularly relevant when a new data process, system or technology is being introduced. Not all new proposed data processing activities will present a high risk to data subjects and a DPIA will not have to be carried out for every project.

DPIAs also support the accountability principle, as they help the Council to comply with the requirements of the General Data Protection Regulation (GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.

Article 35 of the GDPR states:

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

When should a DPIA be conducted?

1. A DPIA should be conducted as early as possible in any new project which ***is likely to pose a high risk to personal privacy*** so that its findings and recommendations can be incorporated into the design of the processing operation.

2. If you are managing any initiative, which may have a high impact on privacy rights, and it involves creating a new process or contract or amending an existing process or contract which uses personal data you must contact the Data Protection Officer (DPO) to begin the DPIA process.

3. If you are managing an initiative which requires a DPIA, you must begin the DPIA process in the planning phase of any project cycle or new contract.

Who is responsible for drafting the PIA?

4. The owner of the process being considered under a DPIA is responsible for drafting the DPIA.

What is the purpose of a DPIA?

5. A DPIA will identify all the privacy risks presented by the project and identify the proposed mitigations to minimise the intrusions on privacy. Known as ***'privacy by design***', the embedding of a data privacy impact assessment into the design of projects can have the following benefits:

- Potential privacy impacts are identified at an early stage and problems can be addressed when it will usually be quicker, simpler and less costly to resolve;
- Actions are less likely to be privacy intrusive and have a negative impact on individuals;
- Awareness of privacy and data protection will increase across the Council;
- The Council will be less likely to breach the GDPR;
- Demonstrate compliance with the Information Commissioner's Code of Practice supporting compliance with data protection legislation - which may be viewed at:

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Procedure for conducting a DPIA

6 If your initiative/project requires technical IT support, contact the IDS manager in the first instance.

7. Once you have identified that high risk personal data will be involved in your proposed project/contract, you should contact the DPO for an initial discussion around your proposals and to run through the DPIA form.

8. If in doubt about the progress or status of your DPIA or of you require advice on completing the from, contact the DPO.

9 Each DPIA will be reviewed by the DPO and proposals reviewed to assess with the process owner risks and consider suggestions for risk mitigation and approval of the DPIA once sufficient mitigation has been demonstrated.

Who approves a DPIA?

10. In every case a DPIA must be reviewed and approved by the Head of Service and the DPO.

Monitoring, Review and Record Keeping

11. The DPO will monitor performance against this Policy and report to the Senior Information Risk Officer on areas for improvement.

12. The DPO will review DPIA's :

- To audit the quality of the process; and
- To ensure the requirements identified have been fully implemented and that all recommendation have been adopted

13 The DPO will keep a central record of DPIA's for audit and reference/precedent purposes.

10. A DPIA may arrive at an outcome that the proposals in an initiative are not appropriate due to the degree of risk to the Council of breaching data protection legislation. In such instances, the DPO will suggest possible alternatives, but may refuse to approve the proposal. If work has already begun on implementing the proposal and contractual arrangements have been entered into before being approved under a DPIA, this would represent a breach of this policy. This may result in the discontinuance of work already commenced and present the Council with legal and financial consequences.

11. The approval of a DPIA is the authorisation that the Council is satisfied that the risks of the proposal are acceptable. This policy is breached by implementing a proposal involving personal data processing, within the meaning of art 35 GDPR without prior DPIA approval, rather than only in the event of something going wrong.

12. The DPO can provide advice on what the DPIA needs to include but cannot complete the form on your behalf.

October 2020