HERTSMERE BOROUGH COUNCIL

Meeting name & Date	**EXECUTIVE** **11 November 2020**
Agenda item	**8.4**
Report title	**Approval of Revised Data Protection Policies**
Report reference no.	EX/20/64
Wards affected	All wards
Report author, job title & email	Harvey Patterson, Head of Legal& Democratic Services harvey.patterson@hertsmere.gov.uk
List of Appendices	Appendix 1 - Draft Revised Corporate Data Protection Policy (To follow) Appendix 2 - Draft Data Protection Impact Assessment Policy Appendix 3 - Draft Staff Data Protection Training Policy Appendix 4 - Draft Special Category, Sensitive and Criminal Offences Data Policy
Reason for urgency	N/A
Is it a Key Decision?	No
Call-in expires on	16 November 2020
Exempt from Call-in	Not applicable
Portfolio Holder	Councillor John Graham Portfolio Holder for Finance and Property

PUBLIC REPORT - this report is available to the public.

1 RECOMMENDATION

1.1 That the Executive approves and adopts for immediate use :-

1.1.1 The draft revised Corporate Data Protection Policy set out in Appendix 1 to the officer's report.

1.1.2 The draft Data Protection Impact Assessment Policy set out in Appendix 2 to the officer's report

1.1.3 The draft Staff Data Protection Training Policy set out in Appendix 3 to the officer's report.

1.1.4 The draft Special Category, Sensitive and Criminal Data Policy set out in Appendix 4 to the officer's report.

2 PURPOSE OF THIS REPORT

2.1 To recommend the approval and adoption by the Executive of revised and new polices intended to ensure compliance with the General Data Protection Regulations 2016 (GDPR) and the Data Protection Act 2018 (DPA).

3 REASONS FOR RECOMMENDATIONS

3.1 An internal audit of the Council 's compliance with GDPR/Data Protection Requirements has identified the need to revise the Corporate Data Protection Policy and to produce a number of other Policies intended demonstrate conformity with the 'accountability' principle introduced by the GDPR. In summary, this principle requires data controllers such as the Council not only to comply with the requirements of the GDPR but also to be able to demonstrate such compliance.

3.2 Moreover, in the event of a serious data breach the Information Commissioner would take into account in determining whether to take enforcement action, including the imposition of a monetary penalty, the degree to which the Council can demonstrate conformity with the accountability principle. In summary, Data Controllers who cannot demonstrate substantial compliance with GDPR/DPA requirements can expect to be fined or have a higher fine imposed and as members will be aware, in the case of a serious privacy breach the Information Commission can levy fines of up to 20 million euros or 4% of annual turnover, whichever is the greater.

Corporate Data Protection Policy

3.3 This is the Council's over-arching data protection policy and is a revision and up-dating of the current policy on the Council's web-site.

Data Protection Impact Assessment Policy

3.4 The adoption of this Policy will assist the Council in complying with its 'privacy by design' obligations under the GDPR. The objective of this principle is to ensure that when data controllers are implementing new business processes or significantly re-designing an existing business process, that data privacy is considered and 'designed-in' at the system specification and configuration stages by means of the formulation and use of a Data Protection Impact Assessment (DPIA). Among other things, a DPIA will seek to identify the legal basis for collecting and processing personal information and enables consideration to be given to minimising the amount of personal data collected as well as to the technical and organisational measures that will be taken to ensure the security and accuracy of such data and that it will be processed fairly and lawfully in accordance with the rights of data subjects.

Staff Data Protection Training Policy

3.5 This policy has be drafted in consultation with HR and sets out the Council's commitment to staff training to ensure that staff are aware of their obligations under the GDPR/DPA.

Special Category, Sensitive and Criminal Data Policy

3.6 Special Category and criminal offence data together comprise the most sensitive personal data where security breaches will always be regarded as serious and require reporting to the ICO. Consequently, this Policy is intended to ensure that the processing by the Council of special category data and criminal offence data is lawful and complies with GDPR/DPA requirements.

3.7 Special category data is defined in Article 9 of the GDPR as personal data revealing:

3.7.1 Racial or ethnic origins;

3.7.2 Political opinions;

3.7.3 Religious or philosophical belief;

3.7.4 Trade union membership;

3.7.5 Genetic data;

3.7.6 Biometric data for the purpose of uniquely identifying a natural person;

3.7.7 Data concerning health;

3.7.8 Data concerning a natural person's sex life or sexual orientation;

3.8 Article 10 of the GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'. In this regard, the Council processes criminal offence data for the purposes of preventing, investigating and detecting fraud and other criminal offences as well as obtaining and processing CRB checks for safe-guarding purposes.

Conclusions

3.9 The approval and adoption by the Executive of the draft policies appended to this report will not only respond to recommendations of the internal auditor but more importantly, will better enable the Council to demonstrate compliance with the accountability principle. In addition, in the case of the draft Special Category, Sensitive and Criminal Data Policy, the adoption of the policy will support the Council in the prevention and detection of and the prosecution of offenders as well as enabling the Council to process Criminal Records Bureau checks for safe-guarding purposes.

4 ALTERNATIVE OPTIONS

4.1 The Executive could decide not to approve and adopt the policies appended to this report. This not recommended because it could prejudice the Council's safeguarding responsibilities as well as placing the Council at increased risk of substantial fines in the event of a serious data breach, taking into account that under the GDPR the Council is required to report such breaches to the ICO no later than 72 hours of becoming aware of their occurrence.

5 FINANCIAL AND BUDGET FRAMEWORK IMPLICATIONS

5.1 No direct costs arise out of the adoption of these policies. However, a failure to adopt them could result in the Council facing increased fines in the event of a serious data protection breach.

6 LEGAL POWERS RELIED ON AND ANY LEGAL IMPLICATIONS

6.1 The Council is required to comply with the requirements of the GDPR/DPA and the adoption of these policies will assist in the fulfilment of that obligation.

7 EFFICIENCY GAINS AND VALUE FOR MONEY

7.1 The use of Data Protection Impact Assessments will enable the Council to design in data privacy considerations when procuring new systems or services or re-designing existing systems or services.

8 RISK MANAGEMENT IMPLICATIONS

8.1 The adoption of these policies will assist in minimising the risk of enforcement action by the ICO including the imposition of financial penalties.

9 PERSONNEL IMPLICATIONS

9.1 None for the purposes of this report.

10 EQUALITIES IMPLICATIONS

10.1 None for the purposes of this report.

11 CORPORATE PLAN AND POLICY FRAMEWORK IMPLICATIONS

11.1 The proper management of personal data will contribute towards the Corporate Action Plan objective of ensuring that GDPR legislation is being correctly applied

12 ASSET MANAGEMENT IMPLICATIONS

12.1 None for the purposes of this report.

13 HEALTH AND SAFETY IMPLICATIONS

13.1 None for the purposes of this report.

14 BACKGROUND DOCUMENTS USEDTO PREPARE THIS REPORT

Document Title:	**Filed at:**

15 CONSULTATION ON DRAFT REPORT

15.1 A draft of this report was sent to the following on the following dates:

Consultee	**Report sent**	**Comments rcvd**
Managing Director	23 October 2020	
Executive Director	23 October 2020	
Head of Finance and Business Services	23 October 2020	
Head of Legal & Democratic Services	Author	
Head of Asset Management	23 October 2020	
Head of Partnerships and Community Engagement	23 October 2020	
Portfolio holder Finance and Property		