Executive Report

Ward(s) affected: Not applicable

Report of Strategic Services Director

Author: Ciaran Ward, Information Governance Officer

Tel: 01483 444072

Email: Ciaran.Ward@guildford.gov.uk

Lead Councillor responsible: Joss Bigmore

Tel: 07974 979369

Email: joss.bigmore@guildford.gov.uk

Date: 24 August 2021

# Amendments to Privacy & Data Protection Policy

**Executive Summary**

This proposal seeks to amend the Council's Privacy & Data Protection Policy (last amended 2018) in the form of an additional section to cover electronic payment procedures, to promote Payment Card Industry Data Security Standards (PCI-DSS) compliance, to reflect new protocols around ICT usage and security and a number of other minor changes.

**Recommendation to Executive**

That the Executive approves the amendments to the Council's existing Privacy and Data Protection Policy, as set out in Appendix 1 to this report.

Reason for Recommendation:
To ensure compliance with Payment Card Industry Data Security Standards (PCI DSS), thereby reducing risk of financial and/or reputational damage.

**Is the report (or part of it) exempt from publication?** No

## 1. Purpose of Report

1.1 This report seeks to amend the Council's Privacy & Data Protection Policy (last amended 2018) in the form of an additional section to cover electronic payment procedures, to promote Payment Card Industry Data Security Standards (PCI-DSS) compliance and to reflect new protocols around ICT usage and security.

1.2 Approval is sought from the Executive for the changes to be implemented.

## 2. Strategic Priorities

2.1 To promote secure financial transactions and compliance with applicable legislation.

## 3. Background

3.1 The Information Commissioner's Office (ICO) General Data Protection Regulation (GDPR) guidelines set out compliance standards required for electronic debit or credit card payments.

3.2 The Payment Card Industry Data Security Standards (PCI-DSS) outlines a number of specific technical and organisational measures that the payment card industry considers applicable whenever such data is being processed.

3.3 If an organisation processes card data and suffers a personal data breach, the ICO will consider the extent to which it has implemented measures that PCI-DSS requires - particularly if the breach relates to a lack of a particular control or process mandated by the standard.

3.4 It was therefore agreed that Council should as a minimum set out such measures in a formal document. In the absence of a stand-alone policy, it was decided that the measures should be outlined within the Council's Privacy and Data Protection Policy.

3.5 The PCI DSS is a set of requirements designed to ensure that organisations which process, store or transmit credit/debit card information maintain a data secure environment. Payment cards and transactions will contain confidential personal data which can include but is not limited to the name on the face of the card, the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, CVC2), and any form of magnetic stripe data from the card (Track 1, Track 2).

3.6 Card payment transaction data stored, processed or transmitted by the Council and/or its authorised contractors/service providers must be protected. Security controls must conform to the PCI DSS standard. All individuals or organisations involved in storing, processing or transmitting personal data through payment cards must therefore comply with the Council's Privacy and Data Protection Policy to ensure the security of this information associated with payment cards and transactions.

3.7 The proposed amendments to the policy (see Appendix 1 section 6, page 10) section will oblige any officer of the Council commissioning goods and/or services on the Council's behalf to notify the Procurement Team if the procurement will result in payment transactions in addition to the payment for the goods/services. The Procurement Team and/or the Data Protection Team may require any contractor/service provider to undertake a Data Privacy Impact Assessment (DPIA) to ensure that such transactions are PCI DSS compliant.

3.8 The added section would therefore act as the lead-in point for the Procurement team to ensure the necessary questions are asked at Selection Questionnaire stage and ensure a DPIA is completed. Similarly, the Legal team must ensure

the contracts are amended to require PCI DSS compliance on an “as required” basis.

3.9 A number of other changes have also been added, including how the policy relates to the Council’s Corporate Plan 2021-25, the measurement and impact of the policy through the annual report to Corporate Governance & Standards Committee and hyper-links to related documentation.

## 4. Consultations

4.1 Following recommendations from Legal and subsequent consultations with the Council’s Information Risk Group, it was agreed to formalise the policy amendments.

## 5. Key Risks

5.1 The proposed amendments will reduce to the risk to the Council of suffering financial penalties and/or reputational damage in the event of a data breach related to card payment transactions.

## 6. Financial Implications

6.1 Not applicable

## 7. Legal Implications

7.1 Article 32 of the GDPR obliges the controller and the processor of the data to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The additional sections in the policy aim to comply with this.

## 8. Human Resource Implications

8.1 Not applicable

## 9. Equality and Diversity Implications

9.1 This duty has been considered in the context of this report and it has been concluded that there are no equality and diversity implications arising directly from this report.’

## 10. Climate Change/Sustainability Implications

10.1 Not applicable.

## 11. Summary of Options

11.1 Not implementing the proposed changes to the policy would put the Council in a dangerous situation in the event of a data breach related to electronic card payment information if no clear measures are set out in a policy document which binds officers of the Council and/or the Council’s contractors.

. The absence of a written policy may therefore constitute a breach of the GDPR.

## 12. Conclusion

12.1 It is proposed to add an additional section to the existing Privacy and Data Protection Policy for the reasons outlined above.

## 13. Background Papers

None.

## 14. Appendices

Appendix 1: Copy of Privacy and Data Protection Policy with additional sections included as tracked changes