LICENSING, AUDIT AND GENERAL PURPOSES COMMITTEE
26 NOVEMBER 2018 **AUDIT MANAGER**
REPORT NO. AUD1807

INTERNAL AUDIT – DATA PROTECTION BREACH POLICY

SUMMARY:
A data protection breach policy has been updated to meet the new General Data Protection Regulation (GDPR) and a form has also been developed to record all data breaches.

RECOMMENDATION:
Members are requested to approve the data protection breach policy

1 INTRODUCTION

1.1 The current data protection breach policy (titled the security incident policy) in place is out of date and required updating to meet the new General Data Protection Regulation (GDPR) and reporting requirements to the Information Commissioner's Office (ICO).

1.2 A data protection breach policy is required to ensure that any data breaches, whether paper or electronic, are dealt with appropriately and the necessary action is taken to mitigate the risk, and where necessary inform individuals and regulatory bodies e.g. the ICO or National Cyber Security Centre.

2 BACKGROUND

2.1 A security incident policy current exists, to deal with data protection breaches, however it is out of date. It was identified by the GDPR working group that the policy required updating.

2.2 The policy has been reviewed by the Legal Services Manager and the IT Network Manager.

3 DATA PROTECTION BREACH POLICY

3.1 A data protection breach policy has been developed to meet the GDPR requirements and ICO reporting requirements. The policy is contained within Appendix A.

3.2 The data protection breach policy details:

- What is personal data,
- What is a personal data breach
- Reporting of breaches

3.3 A flow chart of action to be taken upon knowledge of a data breach has been developed and included within the policy.

3.4 The ICO require data breaches to be recorded, whether the ICO is required to be notified or not. A form has been developed and included within the policy to ensure that the necessary data is recorded. A log of all data breaches will be held by the Data Protection Officer.

3.5 Failing to correctly notify the ICO of a data breach can result in a significant fine for the Council.

4 ROLL OUT TO EMPLOYEES AND MEMBERS

4.1 The policy will be communicated to staff and Members via the staff hub with a link to the relevant page on inform. A session will also be held at middle managers meeting to highlight the key issues and actions to be taken. This can then be cascaded down to all employees and Members.

4.2 The communication of the policy to new employees will be carried out during their induction session.

AUTHOR: Nikki Hughes, Audit Manager
01252 398810
nikki.hughes@rushmoor.gov.uk

HEAD OF SERVICE: Peter Timmins, Interim Executive Head of Financial Services

References:
ICO website
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/