REPORT of
DIRECTOR OF RESOURCES

to
FINANCE AND CORPORATE SERVICES COMMITTEE
6 MARCH 2018

INFORMATION SECURITY INCIDENT REPORTING & DATA BREACH MANAGEMENT POLICY

1. PURPOSE OF THE REPORT

1.1 To consider the draft Information Security Incident Reporting & Data Breach Management Policy, attached as **APPENDIX 1** to this report, and recommend the adoption of this policy to the Council.

2. RECOMMENDATIONS

To the Council

That the Information Security Incident Reporting & Data Breach Management Policy, attached at **APPENDIX 1,** be approved.

3. SUMMARY OF KEY ISSUES

3.1 The Introduction of the General Data Protection Regulations (GDPR) bring with it requirements to ensure that all organisations have appropriate security procedures in place, along with policies and practices to deal with any data breaches.

3.2 This policy has been created as an integrated document that deals with both Information & Communications Technology (ICT) incidents and physical data breaches via a single methodology.

3.3 GDPR introduces new timeframes in which a security breach must be report to the Regulator – the Information Commissioner's Office (ICO). Incidents must now be reported (where applicable) with 72 hours of becoming aware of such an incident.

3.4 The Policy seeks to ensure:

- A consistent approach to all security incidents and/or data breaches across the Council;
- The ability to respond quickly and minimise the impact of any such events;
- Compliance with our obligations to report incidents to the Regulator within 72 hours;
- Create a documented record of such incidents for investigation of the circumstances and creating recommendations for future improvement activity;

4. CONCLUSION

4.1 To approve this policy which creates a single policy for dealing with all data security matters, by adopting it the Council will have a robust procedure for dealing with all such events.

5. IMPACT ON CORPORATE GOALS

5.1 Whilst this is an internal procedural policy, by having such arrangements in place it helps support the aims to deliver good quality, cost effective and valued services.

6. IMPLICATIONS

(i) **Impact on Customers** – This policy has no effect on customers. It is an internal procedural policy only. By having good arrangements in place, our customers data should be well protected and managed.

(ii) **Impact on Equalities** – This policy has no effect on equality issues.

(iii) **Impact on Risk** – This policy should reduce and mitigate against risks associated with MDC's data handling processes, and minimise any potential impacts of any such security incidents or breaches.

(iv) **Impact on Resources (financial)** – No direct impact on resources. By utilising the protocols within this policy, any potential sanctions for the Council by the Regulator would be minimised if there were to be a data or security breach.

(v) **Impact on Resources (human)** – No negative impact on resources.

(vi) **Impact on the Environment** – No negative impact on the environment.

Background Papers:

Appendix A: Information Security Incident reporting & Data Breach Management Policy

Enquiries to: Emma Foy, Director of Resources, (Tel: 01621 875762).