
TITLE: Information Security Policy 2020

Committee: Finance & Assets Committee

Date: 6th February 2020

Author: Karen Wright, ICT Manager

[U173]

1.0 ISSUE

1.1 To consider and approve the Council's Information Security Policy 2020.

2.0 RECOMMENDATION(S)

2.1 Members are requested to:

- i) Approve the Information Security Policy as set out in Appendix 1; and
- ii) Delegate authority to the Corporate Management Team to approve any Codes of Practice arising from this policy.

3.0 BACKGROUND/OPTIONS

3.1 The Council last refreshed the Information Security Policy in 2016. Since this last refresh there have been changes in legislation that require the need for a new policy to be considered and approved.

3.2 The Information Security Policy (provided at Appendix 1) provides a framework and guidance to ensure that all data held by the Council, in any format, is secure and complies with the requirements of the relevant legislation, particularly the Data Protection Act 2018.

3.3 It is important to note that the Information Security Policy should not be read in isolation. Users of the policy must read the Information Security Policy in conjunction with other policies, codes of practice and guidance documents.

4.0 ARGUMENTS/CONCLUSIONS

4.1 The Information Security Policy provides clear and defined guidelines that must be followed by staff, third party contractor and elected Members. Without these clear guidelines the Council could be at risk of data breaches.

4.2 It is intended that this policy will be reviewed in three years time, unless there are changes to legislation that requires the policy to be reviewed sooner.

4.3 In addition to this policy there will be a need to develop Codes of Practice documents. These documents will provide information about the practical application of the themes referred to in the policy. As with the Health & Safety

Codes of Practice, these will be approved by the Corporate Management Team and published on the Intranet.

5.0 FINANCIAL IMPLICATIONS

5.1 There are no additional financial implications arising from this report.

6.0 EQUALITY IMPACT ASSESSMENT/CARBON IMPACT ASSESSMENT

6.1 An Equality Impact Assessment is not required.

6.2 A Carbon Impact Assessment is not required.

7.0 APPENDICES

7.1 Appendix 1- Information Security Policy (2020)

<u>Background Documents</u>	<u>Location</u>	<u>Contact Officer</u>
Information Security Policy Manual (June 2016)	The Grange, Ely	Karen Wright ICT Manager (01353) 665555 E-mail: karen.wright@eastcambs.gov.uk