Aberdeenshire COUNCIL Business Services

REPORT TO BANFF & BUCHAN AREA COMMITTEE – 18 AUGUST 2020

INFORMATION SECURITY POLICY AND ASSOCIATED PROCEDURES

1 Reason for Report / Summary

1.1. The purpose of this report is to seek Members' comments and feedback on a new Information Security Policy, a new Mandatory Operating Procedure covering the acceptable use of IT and a new Mandatory Operating Procedure covering Information Asset Management.

2 Recommendations

The Committee is recommended to:

2.1 Review and provide comments to Business Services Committee on the following Policy and Mandatory Operating Procedures:

- **Appendix 1: Information Security Policy**
- **Appendix 2: Mandatory Code of Practice: Acceptable Use (ICT)**
- **Appendix 3: Mandatory Code of Practice: Asset Management**

2.2 Provide comment to Business Services Committee on the proposal:-

- **To grant delegated powers to the Head of Service (Customer & Digital) to make changes and revisions to the Information Security Policy to ensure it remains accurate, relevant and fit for purpose for as long as such changes and revisions do not significantly alter the meaning or essence of the Policy.**

- **To revoke the following policies currently in force:**

  - **Information Security Police**
  - **Acceptable ICT Use Policy**
  - **ICT Asset Management Policy**

- **To approve the following Policy and Mandatory Operating Procedures:**

  - **Appendix 1: Information Security Policy**
  - **Appendix 2: Mandatory Code of Practice: Acceptable Use (ICT)**
  - **Appendix 3: Mandatory Code of Practice: Asset Management**

3 Purpose and Decision Making Route

3.1 Aberdeenshire Council provides access to a range of IT services and facilities which are vital for the delivery of Council services. To ensure the appropriate and effective use of these, IT has developed a number of policies, procedures and guidance covering all aspects of IT use.

3.2 The documents before the Committee have undergone consultation with key managers and Trade Unions and form part of a wider newly introduced Information Security Framework providing practical guidance to Elected Members, staff including teachers, visitors, any third parties engaged to support Council activity and who have authorised access to any Council information assets.

3.3 To reflect the accelerating pace of change in the use and application of technology across the Council, and to meet the requirements of Internal Audit Report 1932 *“Data Security in a Cloud Based Environment”* it was necessary to improve the currency and relevance of a number of existing policies, guidance and code of practices leading to the introduction of a set of new documents which consists of a single overarching policy definition supplemented by various rules governing computer use.

3.4 In terms of information and cyber security, a proactive and preventive approach is needed in order to properly safeguard the Council’s information assets and protecting it from both external and internal threats. In order to ensure that the Council’s Information Security Policy remains current and reflective of technological developments, it would be appropriate and reasonable in all the circumstances to grant the Council’s Head of Service (Customer & Digital) delegated powers to allow the post holder to make changes to the Policy in order to ensure that it remains current and relevant. Such changes would subsequently be communicated to all relevant stakeholders via established HR & OD processes.

3.5 It is recognised that operating procedures are organisational processes with no need for committee approval. However, as the new operating procedures (Appendix 2 and Appendix 3), make reference to, and apply to, Councillors, is preferable to seek members’ comments and feedback prior to implementation.

4 Discussion

4.1 Information is the Council’s most valuable asset - whether it relates to customers, employees, business processes or services – and the onus is on the Council to take a responsible attitude to its critical information.

4.2 Protecting our information is at the heart of being a trustworthy Council, and it is, therefore, essential that we have a robust Information Security Policy and associated procedures in place which allow us to instil confidence in our approach to information and cyber security.

4.3 The new Information Security Policy and associated procedures clearly set out the processes by which the Council has to abide while taking the necessary steps to ensure that the its information and cyber security risks are properly managed in order to meet ever shifting needs.

4.4 The new Information Security Policy and associated procedures will reduce risk levels and corporate exposure to vulnerabilities while making sure that anyone with access to IT services and facilities is aware of their responsibilities.

5 Council Priorities, Implications and Risk

5.1 This report helps to support:

- Priority 1: Our People
- Priority 2: Our Environment

5.2 The report is also aligned with the Council`s Digital Strategy through the use of technology to streamline service delivery, reduce demand and remove avoidable contact wherever possible as well as enhancing our digital workplace by providing solid, reliable and innovative technology solutions and facilitating secure access to all appropriate systems and information to allow staff to do their jobs efficiently and effectively.

5.3 The table below shows whether risks and implications apply if the recommendations are agreed.

Subject	Yes	No	N/A
Financial			x
Staffing	x		
Equalities			x
Fairer Scotland Duty			x
Town Centre First			x
Sustainability			x
Children and Young People’s Rights and Wellbeing			x

5.4 An equality impact assessment is not required because this report seeks Committee approval for a new policy and associated guidance applicable across the Council and does not have a differential impact on any of the protected characteristics.

6 Scheme of Governance

6.1 The Head of Finance and Monitoring Officer within Business Services have been consulted in the preparation of this report and their comments are incorporated within the report and are satisfied that the report complies with the Scheme of Governance and relevant legislation.

6.2 The Committee is able to consider and take a decision on this item in terms of Section B.1.2 of the List of Committee Powers in Part 2A of the Scheme of Governance to consider, comment on, make recommendations to Services and any other appropriate Committee on any matter or policy which impacts its Area.

Ritchie Johnstone, Director of Business Services

Report prepared by Lars Frevert, Information Security Assistant
Date 3 August 2020

List of Appendices

Appendix 1: Information Security Policy
Appendix 2: Mandatory Operating Procedure: Acceptable Use (IT)
Appendix 3: Mandatory Operating Procedure: IT Asset Management

From mountain to sea

Aberdeenshire
COUNCIL

APPENDIX 1

Information Security Policy

Version 1.4 (DRAFT)