WEST DUNBARTONSHIRE COUNCIL

Report by Strategic Lead – People & Technology

Corporate Services Committee: 21 August 2019

Subject: Information Security Policy review

1. Purpose

1.1 The purpose of this report is to provide the Committee with an update on the Information Security Policy and secure approval for same.

2. Recommendations

2.1 The Committee is asked to:

2.1.1 Note that there have been significant technological changes since the last review and this required a rewrite to address the changing and emerging threats;

2.1.2 Note that the ICT Security Policy is now a wider framework of documents including:

- Acceptable Use Policy (AUP);
- Acquisition and Disposal of ICT;
- Privacy and Monitoring;
- Information Security - DPA forum charter; and
- Reporting of Information Security concerns.

2.1.3 Approve the revised Information Security Policy and the associated framework documents listed in 2.1.2 above. Please note that the hyperlinks for this framework will be amended to point to intranet versions following approval).

3. Background

3.1 The existing Acceptable Use policy was approved on the 8 May 2013 by the Corporate Services Committee and rolled out thereafter via email, intranet and awareness sessions to employees affected by this policy.

3.2 Minor, technical revisions regarding password security and data sharing were made at the request of service areas in 2015 and 2016 and communicated via email. The Policy is and will continue to be promoted and available via the Council's intranet.

3.3 The requirement to update the policy is captured as part of the internal audit of Data and Information Security - Governance and Practice (action reference T&PSR/IAAP/622 – Update required to Acceptable Use Policy).

3.4 The adoption of a framework approach combined with the revision of the Acceptable Use Policy will make it easier for everyone affected to understand and carry out their roles in relation to the proper governance and use of the Council's ICT Resources.

3.5 The Information Security Policy is significantly aligned to the Records Management policy which is currently under review by Regulatory Services and subject of a future committee paper and includes:

- Records Management guidance; and
- Information Handling and Classification procedure.

4. Main Issues

4.1 Due to the previously mentioned audit action, technological advances and changes to the ICT threat landscape it was deemed a review was required to bring the policy up to date.

4.2 In order to simplify the policy, a framework approach was adopted. This framework approach includes the introduction of specific documents which are subject to change and allows for the main framework document to remain mostly static, for example, disposals was removed from the AUP and included in the guidance document Acquisition and Disposal of ICT.

4.3 This Policy will be supported by corporate procedures and guidance which will set out how employees, elected members and other relevant groups are expected to carry out their roles in relation to the use of ICT Resources.

4.4 Key changes are mainly in the AUP part of the security framework and provide additional clarity and focus. These changes fall under the categories of personal and unacceptable use and can be summarised as follows;

- Prohibiting auto forwarding to personal email accounts;
- Checking email and document sources before opening;
- Using Council resources to only store Council business related data;
- Not sharing IT accounts or account information;
- Locking and password controls on devices when left unattended;
- New process under review for devices returning from use abroad and annual MOT process;
- Restricted access to Bring Your Own Device (BYoD) for some employees based on job role; and
- Additional restrictions on employees undertaking card payment processes.

5. People Implications

5.1 The revised Information Security Policy forms part of the Council's mitigation against the risk that our employees, elected members and other bodies

(partners, suppliers etc.) may encounter when using council technology resources.

5.2 This policy provides the information required by employees, elected members and other groups to develop the necessary knowledge to understand their obligations in the proper use and governance of council and citizen information and data.

6. Financial and Procurement Implications

6.1 There are no financial and no procurement implications to this report.

7. Risk Analysis

7.1 Without an up to date Information Security Policy to mitigate against emerging threats and new technologies, there is an increased likelihood of significant reputational and financial risks for example financial penalties as a result of data breaches.

7.2 This policy is part of a suite of controls to address Strategic risks SR004 (Information Technology) and SR008 (Threat of Cyber attack) included in the Council's strategic risk register.

8. Equalities Impact Assessment (EIA)

8.1 An equalities impact assessment was carried out and there is no adverse impact on any protected group.

9. Consultation

9.1 A working group comprising ICT, Security, Legal and Human Resource colleagues was established to contribute to the overall review. The review was focussed on the technical changes required to ensure compliance. The draft was circulated to the Strategic Leadership Group and Trades Unions for comment.

10. Strategic Assessment

10.1 High quality technologies and services contribute to the Council's strategic priority of delivering fit for purpose estate and facilities.

Name: Victoria Rogers
Designation: Strategic Lead - People and Technology
Date: 6 August 2019

Person to Contact: Brian Miller, ICT Section Head Infrastructure
07876397925

brian.miller@west-dunbarton.gov.uk

Appendix: Information Security Policy
Acceptable Use Policy (AUP)
Acquisition and Disposal of ICT
Privacy and Monitoring
Information Security - DPA forum charter
Reporting of Information Security concerns

Background papers: none

Wards Affected: All