Aberdeenshire COUNCIL Business Services

REPORT TO BUSINESS SERVICES COMMITTEE – 2 MARCH 2017

DATA PROTECTION POLICY STATEMENT

1 Recommendations

The Committee is recommended to:

1.1 Approve the attached revised Data Protection Policy Statement at Appendix A.

2 Background / Discussion

2.1 A review of the terms of the Data Protection Policy Statement has been undertaken both in terms of a general review and to include a new provision, at Section 11, requiring staff who process personal data to undertake mandatory Data Protection awareness training, and refresher training, as recommended for consideration within Internal Audit Report Data Protection (Report No. 1712).

2.2 The requirement for staff to undertake Data Protection awareness training, and refresher training, was formally agreed by the Chief Executive in an undertaking to the Information Commissioner's Office following a previous contravention of the Data Protection Act.

2.3 Henceforth, any member of staff failing to undertake mandatory training will be in contravention of Council policy over and above failing to comply with reasonable management instruction.

2.4 The Head of Finance and Monitoring Officer within Business Services have been consulted in the preparation of this report and had no comments to make.

3 Scheme of Governance

3.1 The Committee is able to take a decision on this item in terms of Section C of the List of Committee Powers in Part 1.1F of the Scheme of Governance as it relates to a policy decision.

4 Equalities, Staffing and Financial Implications

4.1 An equality impact assessment is not required because the recommendations do not have a differential impact on any of the protected characteristics.

4.2 There are no staffing and financial implications.

Ritchie Johnson
Director of Business Services

Report prepared by Andrew Lawson, Principal Information Security Officer
Date 23/01/2017

APPENDIX A

DATA PROTECTION POLICY STATEMENT

1. **Commitment to the Act**
   Aberdeenshire Council supports the objectives of the Data Protection Act 1998 and seeks to instruct all individuals who have access to the Council's personal data to observe its Principles (see Code of Practice: Data Protection Act 1998). The Chief Executive has overall responsibility for the implementation of the Council's policy for Data Protection and each Service Director will retain executive authority for the compliance of employees with the Policy and associated Code of Practice.

2. **Scope**
   This Code of Practice applies to all employees, contractors and any other individuals working with or for the Council who have access to the Council's personal data.

3. **Notification**
   All purposes for which the Council holds personal data on computer must be notified to the Information Commissioner's Office and kept up to date. It is a criminal offence to fail to notify within 28 days of commencing data processing. All computer systems containing personal data must be intimated by the system 'owner' to the Council's Data Protection Officer for inclusion in the notification process. All purposes for which the Council holds personal data in structured manual records may also be notified to the Information Commissioner's Office and kept up to date. Notification of structured manual records is optional.

4. **Contents of computer files and structured manual records**
   The Council will comply fully with the eight Data Protection Principles in holding and processing personal data.

5. **Confidentiality**
   All individuals who have access to the Council's personal data are expected to protect the confidentiality of that data.

6. **Subject Access**
   The Council will respond to any individual who makes a subject access request in the approved manner. A fixed fee of £5 for a request involving access to records held by a single Service and £10 for a request involving access to records held by two or more Services will normally be charged.

7. **Disclosures**
   Disclosure of personal data will be made in accordance with the Council's registration. In certain cases involving crime or taxation, for example, special exemptions to this rule may apply.

8. **Security**
   All individuals who have access to the Council's personal data must comply with the requirements of the Council's Information Security Policy, Acceptable Use Policy and associated Code of Practice: Acceptable Use of ICT Facilities.

9. **Private Use of Computers**
   Any private use of computers belonging to the Council by employees must comply with the requirements of the Council's Information Security Policy, Acceptable Use Policy and associated Code of Practice: Acceptable Use of ICT Facilities.

10. **Discipline**
    Any employee who deliberately breaches the Council's Data Protection Policy will be subject to established disciplinary procedures as set out with the Council's Disciplinary Policy.

11. **Training**

    All employees who have access to the Council's personal data must undertake mandatory Data Protection awareness training within three-months of commencing employment and undertake refresher training every three years thereafter.