Aberdeenshire COUNCIL Business Services

REPORT TO BUSINESS SERVICES COMMITTEE – 14 JUNE 2018

DATA PROTECTION POLICY

1 Recommendations

The Committee is recommended to:

1.1 Approve the General Data Protection Regulation (GDPR) and Data Protection Act (2018) compliant Data Protection Policy, at Appendix A.

2 Background / Discussion

2.1 A review of the terms of the Data Protection Policy has been undertaken both in terms of a general review and to ensure compliance with and readiness for the General Data Protection Regulation (GDPR) and the Data Protection Act (2018) which come into force on 25th May 2018.

2.2 The scope of the Data Protection Policy has been extended to include Elected Members. Where Elected Members process Council personal data they are considered effectively the same as staff. If an Elected Member were to lose or inappropriately disclose Council personal data, the Council could under GDPR potentially receive a fine of up to 20,000,000 Euros. The risk of receiving a fine is higher if Data Protection awareness training has not been provided and undertaken. This policy therefore mandates GDPR awareness training for all staff and Elected Members who process Council personal data.

2.3 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 and are satisfied that the report complies with the Scheme of Governance and relevant legislation.

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 Implications and Risk

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

4.2 There are no direct financial or staffing implications arising from this report.

4.3 The following risks have been identified as relevant to this matter on a Corporate level

- The Council must by law have a Data Protection policy in place

4.4 There are no Town First implications arising directly from this report.

Ritchie Johnson
Director of Business Services

Report prepared by Andrew Lawson, Acting Data Protection Officer
Date 29th May 2018

APPENDIX A

DATA PROTECTION POLICY

1. Commitment to Data Protection legislation

Aberdeenshire Council supports both EU and UK Data Protection law and seeks to instruct all individuals who have access to the Council's personal data to observe its obligations and principles. The Chief Executive has overall responsibility for the implementation of the Council's Data Protection Policy and each Service Director will retain executive authority for compliance with this policy.

2. Scope

This policy applies to all employees, elected members, contractors and any other individuals working with or for the Council who have access to the Council's personal data, including any providers of digital web-based services.

3. Confidentiality

All individuals who have access to the Council's personal data are expected to protect the confidentiality of that data. All Council employees have an implicit duty of confidentiality to the Council. All non-employees, with access to Council personal data, are expected to sign the Council's Confidentiality Agreement.

4. Training

All employees and elected members who have access to Council personal data shall undertake mandatory Data Protection awareness training within three-months of commencing employment, or being elected, and undertake refresher training every three years thereafter.

5. Breaches

Suspected Data Protection breaches shall be reported to the Council Data Protection Officer within 24 hours of identification of the suspected breach, via a Breach Reporting webform located on Arcadia. The Data Protection Officer shall subsequently investigate the breach and where necessary report the breach to the ICO within 72 hours of breach confirmation.

6. Data Protection Officer

Employees shall ensure the Data Protection Officer (DPO) is involved properly and in a timely manner in all issues which relate to the protection of personal data. The DPO shall receive support from Services in carrying out his/her tasks. The DPO role is to inform and advise the Council on its Data Protection obligations and to co-operate with, and act as the contact point, for the ICO.

7. Lawfulness of Processing

Personal data shall only be processed within the Council where at least one lawful condition for processing applies e.g. where an individual has provided their consent to the processing, where processing is necessary for compliance with a legal obligation, where processing is necessary for the performance of a contract, etc.

Special category personal data, e.g. concerning racial or ethnic origin, political opinions, religious beliefs, etc. shall only be processed where in addition at least one lawful special category condition applies e.g. where an individual has provided their

explicit consent, where processing is carried out in relation to obligations of employment, etc.

8. Individual's Rights - Right to be Informed

Where personal data is collected from a data subject, at the time the personal data is obtained, the Council shall provide the data subject with a Privacy Notice. The Council's Privacy Notice Guidance and Template shall be used for this purpose, to ensure all information required by law is provided. Where personal data is obtained from a third party, the Council shall provide the data subject with a Privacy Notice within one month.

9. Individual's Rights - Access Requests

On request, the Council shall provide a copy of an individual's personal data to that individual. This shall be provided free of charge, except where further copies are requested in which case a reasonable fee may be charged. Where a request is made by electronic means, the information shall be provided in a commonly-used electronic format. The information shall be provided without undue delay and in any event within one month of receipt of the request. This period may be extended by two further months, where necessary, taking into account the complexity and number of requests.

10. Individual's Rights – Rectification

On request, the Council shall rectify any inaccurate personal data, or complete any incomplete data, concerning a data subject without undue delay.

11. Individual's Rights – Erasure (Right to be Forgotten)

On request, the Council shall erase the personal data of a data subject where certain conditions apply without undue delay e.g. where a data subject withdraws their consent and there is no other legal ground for processing.

12. Individual's Rights – Restriction of Processing

On request, the Council shall restrict the processing of a data subject's personal data where the accuracy of the data is contested until the Council verifies the accuracy of the personal data.

13. Individual's Rights – Data Portability

On request, the Council shall provide a copy of an individual's personal data to that individual in a structured, commonly-used and machine-readable format. This right only applies where the processing is consent-based or contract-based and the processing is carried out by automated means.

14. Disclosures and Data Sharing

Any disclosure or sharing of personal data will be carried out in accordance with Data Protection law. Where data sharing is routine, i.e. more than ad-hoc, a Privacy Impact assessment shall be undertaken, and a Data Sharing Agreement or Information Sharing Protocol shall be put in place between parties to the agreement.

15. Security

All individuals who have access to Council personal data shall comply with the requirements of the Council's Information Security Policy, Acceptable Use Policy and associated Codes of Practice.

Appropriate technical and organisational measures shall be implemented by the Council to ensure a level of security appropriate to the risk, including as appropriate,

pseudonymisation and encryption of personal data, ability to ensure confidentiality, integrity, availability and resilience of processing, and a process for regularly testing, assessing and evaluating the effectiveness of security measures.

16. Private Use of Council Devices and Bring Your Own Device (BYOD)

Any private use of Council-owned devices, and any Council use of privately-owned devices, shall comply with the requirements of the Council's Information Security Policy, Acceptable Use Policy and associated Codes of Practice.

17. Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment shall be undertaken when using new technologies and where the processing is likely to result in a high risk to the rights and freedoms of individuals. Processing that is likely to result in a high risk includes, but is not limited to, extensive processing activities, profiling, where decisions have legal effect, or similarly significant effect, on individuals, large scale processing of sensitive data or personal data in relation to criminal convictions or offences and large scale, systematic monitoring of public areas e.g. via CCTV.

18. Use of Data Processors

The Council shall only engage the services of a Data Processor which can provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of EU and UK Data Protection law. A contract that is binding on the Data Processor shall be in place that sets out what the Data Processor can and cannot do in respect of Council personal data.

19. International Transfers

The transfer of Council personal data to a third country or to an international organisation shall only take place where that third country or international organisation ensures an adequate level of protection. In general, Council personal data should not be transferred out with the EU. In the case of transfer of personal data to the United States, this shall only be appropriate where the organisation concerned has current Privacy Shield accreditation. For the avoidance of doubt, this applies to providers of digital web-based services.

20. Records of Processing Activities

The Council shall maintain a record of its processing activities. Each Council Service is responsible for ensuring that its Information Asset Register is managed and kept up-to-date.

21. Discipline

Any employee who deliberately or recklessly breaches the Council's Data Protection Policy may be subject to established disciplinary procedures as set out with the Council's Disciplinary policy

22. Processing of Special Category Data

UK data protection law requires controllers who process special category personal data under various parts of the Data Protection Act (2018) to have an "appropriate policy document" in place setting out a number of additional safeguards for this data.

a: Lawfulness, fairness and transparency:

All data flows into and out of the council will be assessed to determine the legal basis under which that data is processed and the results of the

assessment will be documented. We will ensure that we have a valid legal basis for holding the personal data we hold, and that we will also have a valid legal basis for disclosing this personal data to third parties where this happens. Privacy notices have been drafted to comply with GDPR requirements and to reflect the legal basis of processing. Data processor agreements and data sharing agreements are being updated to reflect the new legal requirements.

b: Purpose limitation:
The purposes for which data are collected are clearly set out in the relevant privacy notices.

c: Data minimisation:
In assessing data flows, the council will take the opportunity to assess the need for each of the data fields in question and where superfluous data is being captured, we will stop capturing this.

d: Accuracy:
The council is continually checking data for accuracy and, where any inaccuracies are discovered, these are promptly corrected.

e: Storage limitation:
The council only keeps personal information for as long as necessary. Sometimes this time period is set out in law, but in most cases it is based on business need. We maintain a records retention and disposal schedule, based on the Scottish Council on Archives Records and Retention Schedules which sets out how long we hold different types of information.

Ongoing management of the council's records and information is subject to the provisions of our Records Management Plan, which was developed in terms of the Public Records (Scotland) Act 2011 and approved by the Keeper of the Records of Scotland. It is available online at: http://www.aberdeenshire.gov.uk/council-and-democracy/info-and-records-mgmt/records-management-plan/. The Records Management Plan sets out, in much greater detail, the provisions under which the council complies with its obligations under public records legislation, data protection and information security and is complementary to this policy.

f: Integrity and confidentiality:
The council has an approved Information Security Policy in place. All staff are required to undertake GDPR awareness training and this is refreshed every three years. Our ICT systems have appropriate protective measures in place incorporating defence in depth and the systems are subject to external assessment and validation. We have policies and procedures in place to reduce the information security risks arising from use of hard copy documentation.