Data Protection Policy

Summary Table

Policy Status	***Approved and finalised***
Responsible Officer	*Andy Lawson, Data Protection Officer*
Policy Sponsor	*Ritchie Johnson, Director of Business Services*
Authorised by	*Business Services Committee*
Approval Date	*14th June 2018*
Review Date	*7th June 2021*

1. Policy Statement

Aberdeenshire Council supports UK Data Protection law and statutory guidance and seeks to instruct all individuals who have access to the Council's personal data to observe data protection 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 services.

3. Principles

3.1 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.

3.2 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 at least every two years thereafter.

3.3 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.

3.4 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.

3.5 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 for processing applies e.g. where an individual has provided their explicit consent, where processing is carried out in relation to obligations of employment, etc.

3.6 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.

3.7 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 up to two further months, where necessary, taking into account the complexity and volume of requests.

3.8 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.

3.9 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 basis for processing.

3.10 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.

3.11 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.

3.12 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 Data Protection Impact assessment shall be undertaken, and consideration should be given to putting a Data Sharing Agreement in place between parties to the agreement.

3.13 Security

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

3.14 Private Use of Council Devices and Bring Your Own Device

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, and associated Mandatory Codes of Practice.

3.15 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment shall be undertaken where the processing is likely to result in a high risk to the rights and freedoms of individuals. The level of risk shall be determined by reviewing the DPIA screening questions located within the DPIA template. Processing 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.

3.16 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 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.

3.17 International Transfers

The transfer of Council personal data to a third country shall only take place where that third country ensures an adequate level of protection. Council personal data shall only be stored and accessed from within the UK, EU/EEA, or any other country deemed safe i.e. a country with an adequacy decision. For personal data to be stored or accessed from any other country, the council must undertake appropriate due diligence by undertaking a DPIA with the risk signed-off by a relevant Head of Service. For the avoidance of doubt, this applies to providers of digital web-based services.

3.18 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.

3.19 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.

3.20 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. The Council shall ensure that there is a valid legal basis for processing the personal data, and a valid legal basis for disclosing personal data to any third parties. Privacy notices shall be provided which detail the legal basis for processing.

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

c: Data minimisation:
On collecting personal data, the council will assess the necessity of collecting each data field and will not collect superfluous data.

d: Accuracy:
The council shall regularly check data for accuracy and, where any inaccuracies are discovered promptly correct the data.

e: Storage limitation:
The council shall only keep 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. The Council shall maintain a records retention and disposal schedule, based on the Scottish Council on Archives Records and Retention Schedules which sets out how long different types of information should be held.

Ongoing management of the council's records and information is subject to the provisions of the Council's 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. The Records Management Plan sets out 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 which must be refreshed at least every two years. IT systems must have appropriate protective measures in place incorporating defence in depth and where appropriate the systems should be subject to external assessment and validation.

4. Related Links

Not applicable

5. Index of Documents

a) Policy

Revision Date	Previous Revision Date	Summary of Changes
7th June 2021	7th January 2020	Revised to incorporate changes resulting from EU Exit, Privacy Shield invalidation, changes to Infosec documents, etc.
14th June 2018	5th December 2016	Revised to comply with GDPR and DPA(2018)
5th December 2016	15th May 2015	Training requirement added, as per internal audit recommendation.
15th May 2015	June 2008	Revision and Distribution sections added.

b) Distribution

Name	Title
All employees, elected members, contractors and any other individuals working with or for the Council who have access to the Council's personal data	