Report No: 95/2018
PUBLIC REPORT

CABINET

19 JUNE 2018

DATA PROTECTION POLICIES AND UPDATE

Report of the Director for Resources

Strategic Aim:	Sound Financial and Workforce Planning	
Key Decision: No	Forward Plan Reference: 240518	
Exempt Information	No	
Cabinet Member(s) Responsible:	Mr O Hemsley, Leader and Portfolio Holder for Rutland One Public Estate & Growth, Tourism & Economic Development, Resources (other than Finance and Communications)	
Contact Officer(s):	Debbie Mogg, Director for Resources	01572 758358 dmogg@rutland.gov.uk
	Adele Wylie, Head of Legal and Corporate Governance	01572758154 awylie@rutland.gov.uk
Ward Councillors	N/A	

DECISION RECOMMENDATIONS
That Cabinet: 1. Approves the Data Protection Policies and Procedures as set out in Appendices 1, 2 and 3

1 PURPOSE OF THE REPORT

1.1 This report outlines the new data protection laws which came into force on 25 May 2018. It sets out the steps which the Council has taken to prepare for the new data protection regime and it seeks Cabinet's approval to the new policies which have been introduced as part of the preparatory work.

2 BACKGROUND AND MAIN CONSIDERATIONS

2.1 The General Data Protection Regulation (GDPR) is a European Directive which came into force on 25 May 2018. It creates a new data protection standard that applies to all Member States in the European Union.

2.2 In very broad terms, the GDPR sets out the respective responsibilities of data controllers, such as the Council, data processors who are responsible for processing personal data on behalf of the Council and data subjects who are individuals whose personal data is being processed.

2.3 The GDPR defines 'personal data' as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly.

2.4 The most common examples of personal data are individuals' names, addresses, dates of birth etc.

2.5 A number of very significant changes have been introduced by the GDPR which are summarised in the report.

2.6 The UK Government has introduced a Data Protection Bill which is intended to give domestic effect to the GDPR. The GDPR provides an overall data protection framework and the Bill, once enacted, will fill in a number of gaps in the framework and provide a much more detailed set of statutory provisions which will take effect in the UK. The new Act will have to be read together with the GDPR on the basis that some provisions within the Act will apply where the GDPR is silent and vice versa.

Summary of changes introduced by the GDPR

The Requirement of the Council to appoint a Statutory Data Protection Officer (DPO)

2.7 The DPO is responsible for ensuring that the Council fully complies with the GDPR and the new Data Protection Act (DPA). The DPO is required to have a direct reporting line to the Chief Executive and the Information Governance Officer has assumed this role for the Council. Her statutory duties include:

- informing and advising the Council and its Members and Officers who process individuals' personal data;
- monitoring compliance with the GDPR and DPA and the Council's data protection policies and procedures;
- providing advice in relation to Data Protection Impact Assessments and monitoring their performance;

- acting as the Council's contact point for the Information Commissioner's Office

2.8 The DPO has drafted a Data Protection Policy, a Data Breach Policy and a Retention Policy which are respectively attached as Appendices one, two and three to the report.

Individual Rights

2.9 A key feature of the GDPR is that data controllers such as the Council are required to process individuals' personal data in a transparent manner and therefore it has provided for the following rights for individuals:

- Right to be informed about the collection and use of their personal data;
- Right to request that their inaccurate personal data is rectified;
- Right to request that their personal data is erased. This is also known as
- Right to be forgotten';
- Right to request that the processing of their personal data is restricted;
- Right to data portability which allows individuals to obtain and reuse their personal data across different Council services;
- Right to object to the processing of their personal data;
- Right not to be subject to automated decision making including profiling

2.10 The GDPR has also shortened the right for a person to access their data this timescale to one calendar month and the requirement to pay a fee has been dispensed with. This will place an additional burden on the Council as it is anticipated that there will be an increase in the number of subject access requests made to it.

2.11 Guidance on the Individual Rights has been produced and can be found on the Councils website.

Data Protection Impact Assessments

2.12 Both the GDPR and the DPA require that carrying out a Data Protection Impact Assessment (DPIA) is mandatory in certain circumstances. A DPIA is a process to help identify and minimise the data protection risks of a particular Council project when the processing of personal data is likely to result in a high risk to individuals' interests.

2.13 A Procedure for undertaking a DPIA has been drafted which includes a template for the use of Officers and can be found on the Councils Website. Officers will also have to consider whether there is a need for a DPIA as part of the formal report writing process.

Data Protection Privacy Notices

2.14 The Council is required by law to publish a Privacy Notice. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

2.15 The DPO has drafted a Generic Data Protection Privacy Notice for the Council which can be found on the Council Website. In addition service areas have been provided with privacy notices which they can amend depending on the how they are using the data.

2.16 The DPO has also added Privacy Notices to members profiles on the Council's website so that the public know how they are using their data.

Reporting Data Protection Breaches

2.17 Two very significant changes have been introduced by the GDPR in relation to data protection breaches. The first imposes an obligation on the Council to notify the ICO of a breach within 72 hours of it occurring. Failure to do so may result in a fine of up to 10 million Euros [£8.8m] being imposed on the Council.

2.18 The second change is that the ICO has the power to impose a fine of up to 20 million Euros [£17.6m] if a data protection breach occurs within the Council. A Data Incident Response Policy is attached at Appendix Two of this report.

Document Retention and Destruction Policy

2.19 The Council has a statutory responsibility to retain and destroy all of its records in accordance with the requirements of the GDPR, the DPA and indeed other relevant legislation. 'Data minimisation' lies at the heart of the new data protection regime and both the GDPR and the DPA stipulate that personal data shall not be kept longer by a data controller than is necessary for its purpose. Therefore, a Records and Retention Policy has been devised with the objective of providing guidance in this respect. A copy of this Policy is attached as Appendix Three to the report.

Data Mapping

2.20 A data mapping exercise was conducted throughout the Council. The purpose of this was to try to capture, by categories, details of as much of the personal data that the Council handles and processes as possible. The information which has been obtained has been translated into an Information Asset Register. This register provides comprehensive overview of the personal data which the Council holds which will further evidence the Council's overall compliance with the new data protection regime.

Forms and Contracts

2.21 All forms within the Council have been updated to ensure compliance with the GDPR.

2.22 A process is currently underway to update all supplier contracts. The GDPR specifies that controllers of data must specify how processors of their data use it.

Training and Awareness

2.23 The Council has introduced an e-learning module on the GDPR which is mandatory for all officers in the Council to complete.

2.24 The DPO has also attended a number of staff and management meetings across the Council for the purpose of raising awareness of the requirements of the new data protection regime.

2.25 The DPO also conducted training for elected members and small/medium businesses.

3 CONSULTATION

3.1 Internal services have been consulted with throughout the prepatory work to ensure compliance.

3.2 External suppliers have been consulted with in relation to existing contracts which are required to be varied in accordance with the new legislation.

3.3 A Project Board was established with representatives from all Directorates which has driven the work plan to achieve compliance.

4 ALTERNATIVE OPTIONS

4.1 The GDPR and the Data Protection Bill, will introduce a new data protection regime and standard and the Council, in its capacity as a data controller, has no option other than to fully comply with the new set of laws.

5 FINANCIAL IMPLICATIONS

5.1 There are no direct financial implications arising from the report. However, as set out in the report there are two changes being introduced as part of GDPR, which will potentially have significant financial implications. Failure to report a breach to the ICO will carry a fine of up to £10 million Euros (£8.8m) and data breach fines will be up to 20 million Euros (£17.6m). These are significantly higher than fines under the current regime.

6 LEGAL AND GOVERNANCE CONSIDERATIONS

6.1 Legal implications are contained within the body of the report.

7 EQUALITY IMPACT ASSESSMENT

7.1 An Equality Impact has not been completed and it is not envisaged that there are an equality implications.

8 COMMUNITY SAFETY IMPLICATIONS

8.1 None identified

9 HEALTH AND WELLBEING IMPLICATIONS

9.1 None identified

10 ORGANISATIONAL IMPLICATIONS HUMAN RESOURCE IMPLICATIONS

10.1 None identified

11 CONCLUSION AND SUMMARY OF REASONS FOR THE RECOMMENDATIONS

11.1 The laws on data protection have been overhauled by European and Domestic Legislation and the Council needs to ensure that it is fully compliant with them and to evidence its compliance by having a set of robust policies and procedures in place.

12 BACKGROUND PAPERS

12.1 There are no additional background papers to the report

13 APPENDICES

13.1 Appendix One - Data Protection Policy

13.2 Appendix Two - Data Incident Response Policy

13.3 Appendix Three - Retention and Records Disposal Policy

A Large Print or Braille Version of this Report is available upon request – Contact 01572 722577.