Report No:69/2022
PUBLIC REPORT

CABINET

5 April 2022

INFORMATION GOVERNANCE POLICY REVIEWS

Report of the Portfolio Holder for Finance, Governance and Performance, Change and Transformation

Strategic Aim:	All	
Key Decision: Yes	Forward Plan Reference: FP/171221	
Exempt Information	No	
Cabinet Member(s) Responsible:	Cllr K Payne, Portfolio Holder for Finance, Governance and Performance, Change and Transformation	
Contact Officer(s):	Marie Rosenthal, Interim Deputy Director for Corporate Governance (Monitoring Officer)	01572 827347 mrosenthal@rutland.gov.uk
Ward Councillors	N/A	

DECISION RECOMMENDATIONS
That Cabinet: 1. Approves the amendments proposed to the Council's Information Governance Policies set out at in Appendix 1 – 4.

1 PURPOSE OF THE REPORT

1.1 To ask Cabinet to approve the Council's Information Governance Policies. These comprise the Data Protection Policy, Document Retention and Disposal Policy, the Data Incident Response Policy, and the Regulation of Investigatory Powers Act (RIPA) Policy.

2 BACKGROUND AND MAIN CONSIDERATIONS

2.1 The UK General Data Protection Regulation (UK GDPR) came into force on 1 January 2021. It creates a new data protection standard that applies to the UK following the break from the European Union (EU). It sets out the key principles, rights, and obligations for most processing of personal data in the UK. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679).

2.2 In very broad terms, the UK 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 UK GDPR defines 'personal data' as any information relating to an identified or identifiable person natural person; an identifiable natural person is one who can be identified directly or indirectly. The most common examples of personal data are individuals' names, addresses and dates of birth etc.

DATA PROTECTION POLICY

2.4 Minor changes have been made to the Council's existing Data Protection Policy to ensure that it is compliant with the updated UK GDPR and the Data Protection Act 2018 legislation.

2.5 Throughout, the previously recognised term GDPR has been replaced by UK GDPR to align the policy with standard practice.

2.6 Further, the Data Protection principles which can be found on the Information Commissioners Office (ICO) website have been amended so that they are legally compliant and in line with the independent regulator. The ICO have amended the principles and now set out 7 principles that should guide the approach to processing data. These are: -

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

2.7 Compliance with the spirit of these key principles is a fundamental building block for good data protection practice. It is also key to compliance with the detailed provisions of the UK GDPR.

2.8 It has been agreed that the Monitoring Officer will be the designated Data Protection Officer.

DOCUMENT RETENTION AND RECORD DISPOSAL POLICY

2.9 In the main, the amendments to this policy are not substantial. References to the previously recognised GDPR have been replaced by UK GDPR.

DATA INCIDENT RESPONSE POLICY

2.10 Similarly, the Data Incident Response Policy has been amended to change references of GDPR to UK GDPR.

2.11 Appendix 1 of the policy 'Data Breach Reporting Form' has been replaced by the latest form that is being utilised internally.

REGULATION OF INVESTIGATORY POWERS ACT (RIPA) POLICY

2.12 The Regulation of Investigatory Powers Act 2000 policy has been updated to recognise the change to the Investigatory Powers Commissioner's Office (IPCO). The Officer to the Surveillance Commissioner (OSC) role has been replaced by the Chief Surveillance Commissioner to the Investigatory Powers Commissioner's Office. However, the duties of the Chief Surveillance Commissioner have not changed.

2.13 The Senior Responsible Officer for RIPA in the council is now the **Monitoring Officer** replacing the Deputy Director of Corporate Governance.

2.14 Section 5.2 in relation to Online Covert Activity has been revised and now includes the Home Office's Code of Practice on Covert Surveillance and Property Interference guidance in relation to online covert activity.

2.15 Section 6.3 and 6.4 includes further revised guidance from the government on Juvenile Sources and Vulnerable Individuals acting as Covert Human Intelligence Sources (CHIS) and that the authorisations of a Juvenile / Vulnerable Individual CHIS must be granted by the Chief Executive only in **exceptional circumstances**.

2.16 Section 7.2 in respect of confidential information now includes confidential constituent information.

2.17 Section 7.6 has been altered to set out that both the Applicant and the Authorising Officer who gave the authorisation for directed surveillance should attend the Magistrates Court for the Authorisation to be approved by a Justice of the Peace.

2.18 In the event that the Applicant cannot be present, guidance has been added to state that the Authorising Officer would need approval for rights of audience subject to Section 223 of the Local Government Act 1972.

2.19 Section 13.0 has been modified to include reference to the IPCO Data Assurance Programme which was introduced in 2020 as part of its inspection regime.

3 CONSULTATION

3.1 Internal services have been consulted throughout the preparatory work to ensure that the policies are compliant with recent regulations and legislation.

3.2 A review of the RIPA policy has taken place by benchmarking with best practice to ensure that the policy the council holds is legally compliant with recent developments.

4 ALTERNATIVE OPTIONS

4.1 There are no possible alternative options as the duty of Rutland County Council District Council as a data controller is to be compliant with the legislation in place insofar as the UK GDPR, The Data Protection Act 2018, and the Regulatory Investigatory Powers Act 2000.

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 create significant financial implications in the event of a data breach. Failure to report a breach to the ICO will carry a fine of up to £8.7m and data breach fines will be up to £17.5m. These are significantly higher than fines under the current regime.

6 LEGAL AND GOVERNANCE CONSIDERATIONS

6.1 Legal and Governance Considerations are included in the main body of the report.

7 DATA PROTECTION IMPLICATIONS

7.1 A Data Protection Impact Assessments (DPIA) has not been completed as no personal data has been processed in the review of the policies in this report.

8 EQUALITY IMPACT ASSESSMENT

8.1 An Equality Impact Assessment has not been carried out because the report is only setting out minor changes to existing polices and is not undertaking a major service review.

9 COMMUNITY SAFETY IMPLICATIONS

9.1 None identified.

10 HEALTH AND WELLBEING IMPLICATIONS

10.1 None identified.

11 CONCLUSION AND SUMMARY OF REASONS FOR THE RECOMMENDATIONS

11.1 Following the UK's departure from the European Union, the laws on data protection have been overhauled by 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 (revised)

13.2 Appendix Two – Document Retention and Records Management Disposal Policy (revised)

13.3 Appendix Three – RIPA Policy (revised)

13.4 Appendix Four – Data Incidence Response Policy (revised)

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