HUMAN RESOURCES COMMITTEE

24 SEPTEMBER 2018

REPORT OF THE DEPUTY CHIEF EXECUTIVE

CORPORATE INFORMATION SECURITY POLICY REPORT

(Report prepared by Judy Barker & Sam Wright)

PART 1 – KEY INFORMATION

PURPOSE OF THE REPORT

To adopt the Data Protection and Information Security Policies that will contribute towards corporate legal compliance with the European General Data Protection Regulations and the UK Data Protection Act 2108, which came into force on 25 May 2018.

EXECUTIVE SUMMARY

These policies have been created to provide a statement of corporate compliance and assurance that the Council recognises and meets its obligations in this regard.

This report recommends that the Corporate Information Security Policy and the Data Protection Policy (Appendices A & B to this report) are endorsed and adopted. These policies will replace the existing outdated polices which will then be withdrawn from publication.

The Information Security Policy (Appendix A) is a replacement policy that addresses and correctly reflects the new legislative references and adopt the standard format of other policies. In addition it clearly defines the various roles and responsibilities of our Information Governance structure and our obligations when processing valuable data and using corporate IT services.

Below is a summary of the changes to achieve a legislative compliant Data Protection Policy (Appendix B) :-

- Reinforces the need for us to share data in order to protect the public funds we administer by preventing and detecting fraud;
- Updates the legal Principles to include the need to be transparent about how and why we process personal information;
- Reinforces the need to comply with our corporate retention policy to ensure we do not store information for longer than is necessary for the purpose it was collected;
- Explains the requirement to appoint a Data Protection Officer and what the role involves;
- Supports the need for appropriate security measures, including impact risk assessments;
- Highlights the updated Rights for individuals, such as the right to be informed, right to rectification, etc.
- Identifies the need for a lawful basis or, if none exists, the need to obtain informed and explicit consent for processing; and
- Covers the mandatory reporting of any ‘serious’ data breaches that meet the Information Commissioner’s (ICO) criteria.

RECOMMENDATION(S)
It is recommended that:- **a) The Corporate Information Security Policy (Appendix A) is approved and adopted with immediate effect.** **b) The Data Protection Policy (Appendix B) is approved and adopted with immediate effect.** **c) That delegation be given to the Information Governance Policy Unit to update these policies with any future legislative and/or administrative changes to ensure they continue to be fit for purpose and to meet legal compliance requirements.**

PART 2 – IMPLICATIONS OF THE DECISION

DELIVERING PRIORITIES
Adoption of the new policies will update the existing outdated policies which do not comply with current legislative requirements. These data protection and security policies form two key strands of the Council's IT and our use and secure storage of data in compliance with latest legislation. As such they are integral to the delivery of our stated Corporate Plan priority of "Delivery of high quality, affordable services" and specifically address; transforming the way we work, the IT improvement programme, engagement with the community and improving customer access to services. They are also key to practical delivery of the adopted customer service strategy. From an equality impact assessment perspective the safe storage and legitimate use of sensitive and personal data in compliance with new UK and European data protection legislation clearly relates to all groups equally, and to their benefit.
FINANCE, OTHER RESOURCES AND RISK
The adoption of these new policies does not create any additional funding requirement. Empowerment of minor information governance and IT security policy changes to the Information Governance Policy Unit, chaired by the Portfolio Holder for Finance and Corporate Resources, will reduce the burden and frequency of calling together the HR Committee for minor policy document updates/ revisions and minimise non-compliance risks.
LEGAL
Information security policy refers to the defence of information and/or information systems from unauthorised or unintended access, destruction, disruption or tampering. It is essential that our organisation acts appropriately with the information we obtain, hold and process. Confidentiality, integrity and availability of information must be proportionate and appropriate to maintain services. The Data Protection Act 2018 requires the Council to collect, process, share and dispose of personal information securely and correctly. This Council recognises that the lawful and

correct treatment of personal information is essential to the delivery of successful operations to our customers and maintaining the confidence of the individuals to whom the data relates (internally and externally).

The Council requires all of its employees, elected members and third parties operating on our behalf to comply with this policy and to cooperate with all measures and procedures in place to ensure legal compliance.

OTHER IMPLICATIONS

None.

PART 3 – SUPPORTING INFORMATION

BACKGROUND

May 2018 saw the introduction of new European and UK Data Protection laws to ensure that the privacy rights of individuals continue to be adequately protected in the current climate of digital processing of information, including the processing of biometric and genetic data.

The European General Data Protection Regulation (GDPR) applies to all EU Member States and protects the privacy rights of all citizens of the EU. The Data Protection Act 2018 incorporates all aspects of the GDPR but includes the legal derogations required to address UK law and to protect the rights of UK citizens following its departure from the European Union.

BACKGROUND PAPERS FOR THE DECISION

None.

APPENDICES

Appendix A – Corporate Information Security Policy

Appendix B – Data Protection Policy