REPORT OF THE PORTFOLIO HOLDER FOR ASSETS AND FINANCE

DATA PROTECTION POLICY

EXEMPT INFORMATION
None

PURPOSE
This report provides an updated Data Protection Policy which details the framework within which Tamworth Borough Council will strive to ensure compliance with the requirements of the Data Protection Act 2018.

RECOMMENDATIONS
It is recommended that

1. Cabinet endorse the policy and approve it for immediate implementation and publication.
2. The Data Protection Officer be given delegated authority to make amendments to the Data Protection Policy to reflect changes to future legislative changes.

EXECUTIVE SUMMARY
The previous Data Protection Policy was approved for implementation in 2015 and was amended in 2018 following implementation of the General Data Protection Regulation. At that time it was embedded into the Council's Information Security Policy. Due to further legislative changes the Data Protection Policy has now been further updated.

The council also appointed a new Data Protection Officer in 2019 following the previous post holder leaving the authority. The Data Protection Officer has taken the opportunity to review all information governance policies, procedures and processes and has updated several of these to ensure compliance with legislation.

The policy confirms the Council's approach to data protection and GDPR compliance and sets out the responsibilities of the Data Protection Officer, Elected Members, managers and employees in ensuring the Council continues to act lawfully.

OPTIONS CONSIDERED

No other options were considered as the Council is required to adopt a Data Protection Policy which reflects current legislation. The policy is based on good practice and guidance from the Information Commissioner.

RESOURCE IMPLICATIONS

All staff are expected to operate under the policy in a manner that is compatible with the requirements of the Data Protection Act 2018.

There is an ongoing requirement for training Officers and Elected Members, these costs will be met from existing budgets.

Annual registration with the Information Commissioners Office costs £2900 which continues to be met from existing budgets.

LEGAL/RISK IMPLICATIONS

The policy seeks to ensure that the Council is compliant with the Data Protection Act 2018 and General Data Protection Regulation (GDPR) (EU 2016/679).

EQUALITIES IMPLICATIONS

No specific implications

SUSTAINABILITY IMPLICATIONS

No specific implications

BACKGROUND INFORMATION

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

The Data Protection Act 2018 governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals (data subjects) can have a certain amount of control over their personal data and the way in which it is handled.

Some of the main features of the Act are:

1. All data covered by the Act must be handled in accordance with the six principles:
    - Processing should be lawful, fair and transparent
    - Personal data shall be collected for specified, explicit and legitimate purposes
    - Personal data must be adequate, relevant and limited to what is necessary
    - Personal data shall be accurate and kept up to date
    - Personal data shall be kept for no longer than is necessary
    - There must be appropriate security in place in respect of the personal data
2. The Data Subject has various rights under the Act including the right to be informed about what personal data is being processed.
3. Processing of data, including special categories of data, must be done under a lawful basis
4. The Data Protection Act 2018 deals with criminal offence data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it.
5. There is a principle of accountability of data controllers to implement appropriate technical and organisational measures that include internal data

protection policies, staff training and awareness of the requirements of the Act, internal audits of processing activities, maintaining relevant documentation on processing activities, appointing a data protection officer, and implementing measures that meet the principles of data protection by design and data protection by default, including data minimisation, transparency, and creating and improving security features on an on-going basis.

6. Data protection impact assessments (DPIA's) are carried out as part of the design and planning of projects, systems and programmes.
7. Data controllers must have written contracts in place with all data processors and ensure that processors are only appointed if they can provide 'sufficient guarantees 'that the requirements of the Act will be met and the rights of data subjects protected.
8. Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours of the Council becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the council will notify those individuals concerned directly.

The Information Commissioner is responsible for regulation and issue notices to organisations where they are not complying with the requirements of the Act. The Information Commissioner can prosecute those who commit offences under the Act and to issue fines.

The General Data Protection Regulations place significant obligations on any organisation that handles the data of individuals living in the EU, independent of where the organisation is located. The new regulation is the most significant change in privacy law in twenty-two years and organisations must develop processes and procedures to avoid facing financial penalties.

The General Data Protection Regulations also introduce new obligations on such matters as data subject consent, data anonymization, breach notification, trans-border data transfers, and appointment of data protection officers.

REPORT AUTHOR
Zoe Wolicki – Assistant Director People

APPENDICES
Appendix 1- Data Protection Policy 2020