General Data Protection Regulations (GDPR) Statement of Compliance

On 25 May 2018 GDPR (or equivalent UK legislation) will replace the Data Protection Act 1998. This statement provides information in relation to the Council's compliance with these regulations.

What is the Council doing to prepare for GDPR?

The Council has undertaken a number of actions to ensure it will comply with GDPR from 25 May 2018. In the main actions include (but are not limited to):

- Ensuring staff undertake appropriate training
- Relevant policies and procedures have been amended including the Data Protection Policy, Data Breach Policy, Information Security Policy, Information Sharing Policy, other local policies, etc.
- Services have devised appropriate action plans
- Each service have appointed GDPR champions
- A GDPR working group has been formed which is attended by the GDPR champions

What technical and organisational security measures are in place?

The Council has a number of technical and organisational measures in place including:

- The Council conducts in-house and independent vulnerability assessments on a frequent basis, this is also followed up by proactive monitoring.
- Utilisation of change management methodologies and processes across our ICT service giving us compliance and monitoring reports
- A risk framework to identify potential risks and mitigate the threat they could pose if realised
- Use of an enterprise antivirus products and secure backup and retention technologies across our organisation
- Mobile devices are encrypted and are managed by a mobile device management system
- Our data centres are housed in secure locations with only authorised personnel able to access
- Remote admin access to our environment and data centre access is strictly restricted to key staff within our ICT Service
- We provide internet and classroom monitoring solutions to ensure the usage of the internet complies with internal governance arrangements
- Ensuring that network passwords comply with the councils password management policy for corporate accounts

Data processed by the Council is either stored on secure servers held at Council locations or on secure Microsoft servers located securely in Europe. See link to Microsoft security statement – https://privacy.microsoft.com/en-us/Privacy

Extra details about Microsoft security can be found via the following links:

https://privacy.microsoft.com/en-GB/privacystatement

https://products.office.com/en-us/business/office-365-trust-center-eu-model-clauses-faq

https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses

https://products.office.com/en-GB/where-is-your-data-located?ms.officeurl=datamaps&geo=All

https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located

Appropriate organisational security measures are also in place, in the main these include (but not limited to):

- Training staff in data protection
- Ensuring adequate policies and procedures are in place
- Fit for purpose building security measures

Do we have appropriate information management accreditation?

The Councils IT security, network arrangements and information management services are also audited on a regular basis by various third party organisations.

How does the Council handle personal data?

See the Councils general Privacy Policy on its website.