

REPORT OF THE  
**Chief Executive**  
PART I

**1. GENERAL DATA PROTECTION REGULATION (GDPR)**

- 1.1. The General Data Protection Regulation (GDPR) and a new Data Protection Act will replace the existing Data Protection Act on 25 May 2018. Although GDPR is a piece of European Union legislation, the British Government has confirmed that it will take effect in full, regardless of Brexit.
- 1.2. The use of technology has changed significantly since the original Data Protection Act came into force and one of the main purposes of the new Regulation is to bring privacy legislation up to date, reflecting a world where personal data is collected more widely and the risk of misusing data has increased.
- 1.3. The changes are designed to bring about greater transparency and assurance for the public and place a higher responsibility on organisations to be more accountable and transparent about how they use personal information. The changes will build upon and add to the existing requirements.
- 1.4. All organisations that handle personal information will be required to keep a record of what types of personal information it uses, who it is shared with and how long it retains it. They will also need to be clear about the legal reasons why they use particular personal data and to explain this and more detail about what they will do with the personal data at the point at which it is collected.
- 1.5. The levels of fines that the Information Commissioner will be able to impose for loss of personal information and other breaches of the legislation will increase significantly from £500,000 to a maximum of 20,000,000 euros (£18 million).

**2. IMPLICATIONS FOR THE COUNTY COUNCIL**

- 2.1. The County Council is in a good starting position following the audit inspection of the Information Commissioner's Office (ICO) in November 2016, where it determined that the County Council demonstrated "high assurance" in the handling of personal information and data security.
- 2.2. The County Council is reviewing its processes, systems and contractual relationships to ensure compliance with the new requirements outlined in GDPR.

### **3. IMPLICATIONS FOR ELECTED MEMBERS**

3.1. Elected Members may have access to, and handle, personal information in three distinct and separate ways:

- i) as a consequence of their duties as a County Councillor
- ii) in pursuance of their constituency duties
- iii) as a result of the activities of their political party

#### **3.2. Conducting duties as a County Councillor**

Members are provided with a secure environment from which to undertake their work through the County Council's secure IT network and an individual email address, which are protected by up to date security and firewalls. This is covered under the County Council's registration as a data controller. Members can therefore have confidence that when using their County Council email account within the County Council's IT systems in accordance with its relevant policies, the required security standards will be met when holding personal information received as part of the duties of an elected Member of the County Council.

3.3. In this regard, Members are reminded of the requirements of the County Council's IT Policies, which apply equally to Members and Officers. Members should not use personal or shared email accounts including where relevant, email accounts provided by other Councils, for County Council business. It is not permitted, for example, to auto-forward emails or calendar entries from County Council to non County Council email accounts due to the sensitivity of data held by the County Council, particularly in the case of social care. Further guidance is available via the Guidance Note 'Provision of IT Services to County Councillors', available on the Members Portal.

3.4. Further training for Members on GDPR will be provided at a dedicated Member briefing session on 22 March 2018, to which all Members are encouraged to attend. In addition, as part of the County Council's overall preparation for GDPR, the mandatory e-learning module for Officers is being updated, and Officers will be required to undertake refresher training. As a matter of good governance it is appropriate that Members similarly complete the updated e-learning module. Opportunity will be provided for Members to do this at the March briefing session referred to above. For those Members unable to attend the briefing session, a link will be sent following the briefing for Members to complete the training electronically.

#### **3.5. Conducting constituency duties**

In respect of constituency work, the County Council arranges the necessary registration as a data controller for those Members who wish it, and will continue to do so.

#### **3.6. Party political activities**

In terms of party political work, for example campaigning during a County Council election, it is a matter for individual Member's to take up any data

protection queries or concerns with their respective political party organisations. It is the responsibility of Members to check if their political party is registered.

#### **4. APPOINTMENT OF DATA PROTECTION OFFICER**

- 4.1. Along with all public authorities, the County Council is required to designate one of its officers to carry out the statutory duties of the Data Protection Officer (DPO) pursuant to Articles 37-39 of the General Protection Regulations (GDPR). A further report will be brought to the next meeting of the County Council in May in this regard.

### **RECOMMENDATIONS**

That the County Council:

- a) Notes the implications of GDPR for the County Council and that in the interests of good governance, and agrees that all Members should undertake the revised e-learning data protection module, prior to the introduction of the new Regulation on 25 May 2018.
- b) Agrees that completion of the data protection e-learning module is included as a requirement for new and returning Members as part of the Member Induction Programme, after any County Council elections.