Report to:	**COUNCIL**		
Date:	**4 December 2018**		
Title:	**General Data Protection Regulation (GDPR) & Data Protection Policy Update**		
Portfolio Area:	**Cllr Chris Edmonds**		
Wards Affected:	**All**		
Urgent Decision:	**N**	Approval and clearance obtained:	**N/A**

Date next steps can be taken: **Immediately**

Author: **Darren Arulvasagam** Role: **Data Protection Officer & Group Manager Business Development**

Contact: **Darren.Arulvasagam@swdevon.gov.uk or 01803 861222**

RECOMMENDED

That the Council RESOLVES to:

1. **APPROVE the amended Data Protection Policy as detailed in Appendix A;**
2. **DELEGATE approval of the related codes of practice and protocol documents (as summarised in section 3 of this report) to the Council's Data Protection Officer; and**
3. **NOTE and SUPPORT the approach and progress made towards GDPR readiness by the Information Governance Group.**

1. Executive summary

1.1 On 25 May 2018 new rules came into force in respect of Data Protection – these are referred to as the General Data Protection Regulation (GDPR - EU regulation) and the Data Protection Act 2018 (UK Law).

1.2 This report provides an overview of the key requirements of the GDPR, outlines the approach that the Council has taken and recommends the adoption of an updated policy and associated guidance for the Council.

1.3 In order to be compliant with the new regulations, the Council has undertaken a comprehensive review of its policies, processes and procedures. This has resulted in the need to update the current, adopted policy (see appendix A).

1.4 GDPR places great emphasis on the documentation that the Council must maintain in order to demonstrate accountability. Compliance requires a detailed review of our approach to information governance, data protection and how we collect and process data.

1.5 A series of related codes of practice have also been prepared, which will underpin the work that the Council, its staff and Members will need to adhere to. These codes will be updated on a regular basis and can be viewed on the Council's intranet and ultimately, internet. Responsibility for keeping these documents updated will fall to the Council's Data Protection Officer and, as such, it is recommended that the approval of these documents is delegated to the Data Protection Officer.

1.6 A summary of the codes of practice is shown in section 3 of this report.

1.7 The Council's Overview and Scrutiny Committee considered a version of this report at its meeting on 6 November 2018 and, following a detailed debate, proceeded to recommend approval to the Council of each of the three recommendations outlined above.

2. Background

2.1 Data protection law changed from 25 May 2018. The previous law had been in place for twenty years - since before the use of the internet, emails and cloud storage services. The General Data Protection Regulation (GDPR) is an EU regulation drafted to be fit for purpose in the digital age.

2.2 GDPR is an EU sourced regulation. In the UK, the existing Data Protection Act which was developed in 1995 has been updated to adopt many of the GDPR requirements and is known as the Data Protection Act 2018. This move will ensure that 'Brexit' will necessarily lead to later changes in the law.

2.3 The new regulation enhances the rights of data subjects and gives them more control over what happens with their data. It also allows for financial penalties to be imposed on any organisation that breaches those rights or does not comply with the accountability principle.

2.4 Organisations need to put technical and organisational measures in place to protect data from loss, unauthorised access, etc. and to ensure the rights of data subjects are protected.

2.5 Under the GDPR, the Council is required to appoint a Data Protection Officer. The regulation states that the appointment must be made on an individual's professional qualities and expert Data Protection knowledge, laws and practices. The Data Protection Officer must also have a direct reporting line to the senior tier of management, and be able to act independently of the Council. The Senior Leadership Team appointed the Group Manager, Business Development to this role and specific training has been undertaken to ensure compliance.

2.6 The Council has an Information Governance Group which is responsible for ensuring the Council is compliant with all information regulation and laws (Data Protection Act, Freedom of Information Act, and Environmental Information Regulations, Data Security) as well as ensuring that suitable good practice advice and training is in place for staff. This group of officers meets regularly to monitor progress against plans. The comprises the Data Protection Officer, Monitoring Officer, Case Management Manager, Support Services Specialist Manager, and the ICT Specialist for Information Security.

2.7 The six general principles under the new legislation are:

2.7.1 Personal information shall be processed lawfully, fairly and in a transparent manner.

2.7.2 Personal information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2.7.3 Personal information shall be adequate, relevant, and limited to what is necessary.

2.7.4 Personal information shall be accurate and, where necessary, kept up-to-date.

2.7.5 Personal information shall be retained only for as long as necessary.

2.7.6 Personal information shall be processed in an appropriate manner to maintain security.

2.8 Personal information under GDPR includes:

- an identifier, e.g. a name, email address, phone number
- personal identification numbers, e.g. bank account or national insurance numbers
- factors specific to an individual's physical, physiological, genetic, mental, economic, cultural or social identity. This would include anything relating to a disability
- location data - data that has any kind of geographic position attached to it, e.g. data collected by wireless networks, swipe cards and smart mobile devices that provide location tracking
- online identifiers, e.g. mobile device IDs, browser cookies, IP addresses

2.9 Special Categories of Data are those which are particularly sensitive, e.g. race, ethnicity, political opinion, genetic or health related data and sexual orientation.

2.10 GDPR applies to 'controllers' and 'processors' – the controller says how and why personal data is processed and the processor acts on the controller's behalf. In most cases, WDBC (Officers and Members) is the controller and processor, but in some cases the data is processed by third parties.

2.11 The rights of individuals under the GDPR have seen some significant enhancements. Since May, individuals have:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling

2.12 The biggest change that the Council needed to address is the ability to locate and delete individual's data across all of the Councils systems when legally required under the rules.

2.13 **Subject Access Requests** (SARs). The new regulations mean that we cannot charge for complying with SAR's and we have to comply with the request within a month rather than the previous 40 days allowed. Since January 2018 the Council has received seven SARs.

2.14 **Lawful basis for processing personal data.** For each processing activity that the Council undertakes, the Council needs to identify the lawful basis for the processing. It is important to assess this particularly in light of the right for data to be deleted – if the only lawful basis for processing is 'Consent' then the information must be deleted on request. The lawful basis for processing the information must also be included within the Privacy Notice.

2.15 **Consent.** The Council has reviewed how it seeks, records and manages consent. Consent for the Council processing data must be freely given, specific, informed and unambiguous. Consent must not be inferred. Consent for data processing must be separate for any other terms and conditions in documents, web pages or other data capture means.

2.16 **Children.** For the first time, GDPR brought in special protection for children's personal data. If the Council obtains personal data in respect of children, the privacy notice must be written in a language that children will understand.

2.17 **Data Breaches.** The GDPR introduces a duty to report certain types of data breach to the ICO, and in some cases, to individuals. The Council will only have to report a breach to the ICO where it is likely to result in a risk to the rights and freedoms of individuals. Additionally, where there is a high risk to these rights and freedoms, resulting in potential for discrimination, reputational damage, financial loss, loss of confidentiality, etc. there is an additional requirement for the individual concerned to be notified. Not all breaches need to be reported to the ICO, but the potential breach must be assessed within the first 72 hours.

2.18 **Data Protection by design and Data Protection Impact Assessment.** GDPR makes 'privacy by design' an express legal requirement. It also makes Privacy Impact Assessments mandatory where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals or where there is processing on a large scale of the special categories of data.

2.19 The Council has:

2.19.1 Prepared a compliant General Data Protection Regulation Policy (see Appendix A)

2.19.2 Delivered online training for Data Protection to all employees

2.19.3 Delivered face to face training sessions for Information Asset Owners and key processing staff (60 staff already received training, with regular updates programmed to ELT and SLT)

2.19.4 Prepared an information asset register for all processing activities and identified the lawful basis for such processing

2.19.5 Prepared & communicated an information / training checklist for Members to advise how they should deal with personal data

2.19.6 Updated its Privacy Notices to be compliant with the new regulation & prepared a data protection impact assessment for all relevant areas of data processing – these are viewable on the Council's website

3. Outcomes

3.1 In order to ensure that the Council is compliant, the Information Governance Group commissioned an external "readiness" audit. A GDPR specialist visited the Council and interviewed key officers in order to ascertain priority areas for consideration. An action plan was created to address the points raised in the readiness audit. The first actions completed have been to appoint a Data Protection Officer (the author of this report) and to instigate a review of all of the Council's data protection policies and procedures. The updated policy has been finalised. Updated codes of practice and procedural documents have been produced and these are in the process of being rolled out across the organisation.

3.2 It is requested that delegated authority is given to the Data Protection Officer, in consultation with the Information Governance Group, to finalise and keep updated the codes of practice and procedures relation to GDPR and Data Protection compliance.

3.3 The Codes of Practice can be found on the Council's intranet. In time, these will be published on the Council's website (as appropriate). A communications and training plan will be delivered to ensure staff understand and engage with the new and updated processes and forms. In actuality, there is little significant change from existing working practices. Operationally the Council has been working to the new regulations and following the recommended guidance since before the inception of GDPR, as the Council readied itself for the new legislation.

3.4 The Council has prepared and updated a series of Codes of Practice in accordance with GDPR and the Data Protection Act 2018 – these are the guidelines by which information is obtained, stored, shared and accessed. The following codes of practice have been prepared / updated:

3.4.1 Obtaining Personal Information

3.4.2 Managing Personal Information

3.4.3 Accountability and Governance

3.4.4 Individuals Rights

3.4.5 Disclosures and Information Sharing

3.4.6 Information Security

3.4.7 Privacy and Electronic Communications Regulations

3.4.8 Code of Practice for Elected Members

3.4.9 Security in Procurement

3.4.10 Use of Surveillance Cameras and CCTV

3.4.11 Processing for Law Enforcement Purposes

3.4.12 Law Enforcement Policy Document for Sensitive Processing

3.4.13 Special Category Information Processing Policy Document

3.5 These codes of practice and policy documents are intended to be living documents and will need to be updated as further guidance is received from the Information Commissioners Office. It is therefore recommended that the responsibility for the approval and review of these documents (and the addition of any further relevant codes and documents) is delegated to the Council's Data Protection Officer, in consultation with the Information Governance Group.

4 Options available and consideration of risk

4.1 Members could opt to follow, amend or reject the recommendations.

4.2 The updated Data Protection Policy has been designed to incorporate changes to the law, which came into force during 2018. Adoption of this updated policy will reflect the Council's compliance with this law. Operationally, the Council has already taken steps to ensure compliance. It is not considered that the Council is at risk of non-compliance.

4.3 Delegating approval to finalise the codes of practice will ensure that the Council retains the agility to update its operating procedures in light of changes to working practices, complaints or breaches.

4.4 Since January 2018, eight Data Protection investigations have been undertaken by the Council, two of which have been referred to the ICO for investigation by the complainants themselves. The Council has not considered, based on the regulations, that any of the investigations have warranted reporting to the ICO.

5 Proposed Way Forward

5.1 If the Council approves this report's recommendations and adopts the updated policy and guidance (as shown in Appendix A), officers will finalise the codes of practice and policy documents and ensure these are embedded within the organisation, in order to maintain council compliance with the new act. The existing data protection policy will be replaced with the new policy.

6.0 Implications

Implications	**Relevant to proposals Y/N**	**Details and proposed measures to address**
Legal/Governance	Y	Compliance with the regulations is critical in ensuring that the reputation of the Council is upheld and that the rights of individuals are protected. Our existing Data Protection policy required updating in order to be compliant – this work has been completed and the recommended policy is shown in Appendix A.
Financial	Y	There are no significant financial implications from achieving compliance – however, there is risk of significant financial penalties for non-compliance. At present, resources have been absorbed / pooled from Support Services, Customer First and Strategy & Commissioning to prepare for and implement the new regulations, with no new budget pressures created.
Risk	Y	A significant amount of work has been undertaken to ensure compliance with the regulations. An action plan is in place and is monitored regularly. A project team has been formed which meets regularly, with oversight by the Information Governance Group and SLT. Training has been and will continue to be arranged for individuals at an appropriate level based on their role in the organisation to ensure awareness of the new regulation & the impact that this has on their activities.
Comprehensive Impact Assessment Implications		
Equality and Diversity	N	There are no Equality and Diversity implications. The regulations apply to all individuals equally.
Safeguarding	N	None – Compliance with GDPR has implicit improvement impacts on safeguarding

Community Safety, Crime and Disorder	N	None
Health, Safety and Wellbeing	N	This is implicit with GDPR and will be dealt with through compliance and revised policies.
Other implications	N	Policies will be updated as a result of compliance with GDPR

Supporting Information

Appendices:
Appendix A – Data Protection Policy (2018)

Background Papers: General Data Protection Regulation (GDPR) – Readiness & Impact, presented to Audit Committee, 22nd March 2018