Report to: **Hub Committee**

Date: **22 September 2015**

Title: **Joint Data Protection Policy**

Portfolio Area: **Support Services**

Wards Affected: **All**

Relevant Scrutiny Committee: **Internal**

Urgent Decision: **N**

Date next steps can be taken: **22 September 2015**

Author: **Catherine Bowen** Role: **Community of Practice Lead Specialist (Legal) and Monitoring Officer**

Contact: **Catherine.Bowen@swdevon.gov.uk**

Recommendations:

That COUNCIL be RECOMMENDED:

1. To approve the Joint Data Protection Policy attached at Appendix A and supporting Codes of Practice and documentation at: http://shdcweb.swdevon.lan/article/10247/Data-Protection-Policy

2. Delegation to the Monitoring Officer to make minor amendments to the Codes of Practice and supporting policy documentation to reflect the emerging working practices of the Council.

1. Executive summary

1) The purpose of this report is to bring before Members a revised Joint Data Protection Policy for approval. A Joint Data Protection Policy has been drafted to support the Council's T18 ways of working.

2) The Data Protection Policy needs to be reviewed and updated in order to reflect current legislation and current working practices and a revised Joint Data Protection Policy is attached at Appendix A.

3) The supporting and underpinning Codes of Practice are available on the Council's intranet at: http://shdcweb.swdevon.lan/article/10247/Data-Protection-Policy and comprise the following:

- Guidance on Data Protection
- Data Protection and Elected Members

- Rights of Individuals
- Obtaining Personal Information
- Managing Personal Information
- Disclosing Personal Information and Information sharing
- Data Protection and Procurement
- Information Security
- Use of Surveillance Cameras
- Privacy and Electronic Communications regulations

4) It is important to have an up-to-date Policy to ensure that:

- Compliance with the principles of the Data Protection Act is maintained
- Personal information is well-managed, held securely and that the rights of individuals are respected
- Data protection is integrated into the Council's working practices and information systems from the moment information is collected through to its destruction
- We have effective codes of practice, procedures, staff reporting and training in place to ensure this policy works in practice.

2. Background, Outcomes and outputs

1) The Data Protection Act applies to anyone in the Council who has access to, uses or passes on personal information in their day-to-day work, and applies to personal information that is held by the Council about living, identifiable individuals. It may be automatically processed, such as on a computer, recording device or closed circuit tv system, or on paper such as hand-written meeting notes stored in a folder.

2) The Act comprises eight principles, which require that personal information must be:

   - Fairly and lawfully processed
   - Held only for specified and lawful purposes
   - Adequate, relevant, and not excessive
   - Accurate and where necessary kept up to date;
   - Kept for no longer than necessary;
   - Processed in accordance with the rights of individuals
   - Kept secure, with appropriate security measures taken to prevent the loss, destruction or unauthorised disclosure of the information;
   - Only transferred to countries outside the European Economic Area with adequate protections in place.

3) In adopting an up-to-date Policy and underlying Codes of Practice, the Council can demonstrate that it has a relevant and fit for purpose set of practices and guidelines understood by Members, Officers and the public, which will be consistency applied to ensure compliance with the legislation.

4) Following the T18 restructure it is intended to rollout a programme of training for all staff and Members to ensure understanding of the Data Principles and application of the policy. It is anticipated that this will be on-line training to minimise costs.

5) The Codes of Practice have been prepared over the last twelve months and will require some further modifications to ensure that they reflect the emerging working practices of the Council and it is recommended that these minor amendments are delegated to the Monitoring Officer. Any significant changes will be brought back before Members.

4. Options available and consideration of risk

1) The alternative is to rely on the existing policy which has not been recently reviewed with the consequent risk that it does not reflect all legislative requirements or current best and working practice.

2) It is important that the Policy is regularly reviewed and updated; Data Protection Act breaches may result in complaints to the Information Commissioner's Office and finding of breaches could result in the Council facing monetary penalties of up to £500,000, being publicly named-and-shamed, and would result in the loss of trust from the people we provide services to.

3) For employees, it is a criminal offence to obtain or disclose personal information without the Council's authorisation or consent, and, when providing information in response to a subject access request, if they alter, deface, block, erase, destroy or conceal any information that the requester is entitled to.

4) It is suggested that an annual report is taken to the Audit Committee on the application of the Policy as Audit currently has responsibility for an overview of Data Protection.

5. Proposed Way Forward

1) In order to ensure compliance with the Data Protection Act and to protect the Council and members of the public, it is recommended that Members approve the Data Protection Policy attached at Appendix A together with the supporting Codes of Practice available on the Council's website at: http://shdcweb.swdevon.lan/article/10247/Data-Protection-Policy

6. Implications

Implications	Relevant to proposals Y/N	Details and proposed measures to address
Legal/Governance	Y	The Data Protection Act 1998 sets out legislative requirements to ensure compliance with Data Protection principles to make sure that personal information is well-managed and that the rights of individuals are respected. It is therefore important that the Council has in place effective codes of practice and procedures and that those policies are approved by Members. The Hub Committee is responsible for adopting the Council's Policies (unless otherwise provided for in the Constitution).

Financial	Y	There are no direct financial implications arising from this report but as mentioned in the report, there are serious financial implications if the Council does not comply with the Data Protection Act whereby the Information Commissioner's Office may impose fines up to a maximum of £500,000. There will be ongoing training costs to ensure compliance and understanding but it is anticipated that these will be kept to a minimum through on-line training.
Risk	Y	There are serious risks associated with failing to adopt a current Data Protection Policy which are identified within the body of the report.
Comprehensive Impact Assessment Implications		
Equality and Diversity		Where relevant these have been identified within the Policy documents
Safeguarding		N/a
Community Safety, Crime and Disorder		N/a
Health, Safety and Wellbeing		n/a
Other implications		None

Supporting Information

Appendices:

Appendix A: Data Protection Policy

The underlying and associated Data Protection Policy **Codes of Practice** are available at: http://shdcweb.swdevon.lan/article/10247/Data-Protection-Policy

If Members require copies please contact Member Services