DECISION ITEM

REPORT OF	MEETING	DATE	ITEM NO
RESOURCES DIRECTORATE	FINANCE AND DEMOCRACY COMMITTEE	19 JUNE 2017	6
DATA ASSURANCE POLICY			

PUBLIC ITEM

This item is for consideration in the public part of the meeting.

SUMMARY

The council's Data Assurance Policy sets out how it complies with its obligations under the Data Protection Act 1998, how it ensures data quality and how it classifies data. The existing policy has been reviewed and the report recommends the adoption an updated policy containing a small number of minor changes.

RECOMMENDATION

To adopt the updated Data Assurance Policy as set out in the draft attached to the report.

SUMMARY OF PREVIOUS DECISIONS

Cabinet 16 November 2011: Adopt the new Data Assurance Policy

Cabinet 26 November 2014: Revise and update policy

CORPORATE PRIORITIES	
Spending your money in the most efficient way to achieve excellent services (**Value for Money**)	√
Delivering the services that customers expect of an excellent council (**Clean and Green**)	√
Working with all partners (**Vibrant Economy**)	
To make sure Fylde continues to be one of the most desirable places to live (**A Great Place to Live**)	
Promoting Fylde as a great destination to visit (**A Great Place to Visit**)	

REPORT

1. The Data Protection Act 1998 imposes duties on persons who hold "personal data", as defined in the act. "Personal data" includes many manual records as well as information held on computer systems. The act requires the council to comply with the eight data protection principles in dealing in any way with personal data.

2. In 2011, the council adopted a Data Assurance Policy to replace its previous data protection policy and data quality policy. The policy is intended to assist persons working in the organisation to know how they are expected to deal with personal data, to help provide assurance to external bodies that the council takes its

obligations seriously and is complying with them and to ensure that the council uses and keeps only high quality, reliable and up-to date information. Decisions underpinned by such data are likely to be better decisions than those where the information base is of poor quality, unreliable or outdated.

3. The policy also contains a methodology for classifying data depending on the level of its sensitivity. It encourages a person producing or handling data to consider the level of its sensitivity when it is produced or handled, and promote consistency across the organisation.

4. The Data Assurance Policy was reviewed and refreshed in 2014 and is now due for further review. The updated policy is attached for members to consider. The changes are minor in nature and are detailed below:

Paragraph 3.9

Old text: *'Modern technology makes it easier to access up-to date information and less necessary to keep a local copy of it. For example, it will rarely be necessary to keep a paper copy of a statutory instrument or government circular. The current versions of those documents are readily available online, and consulting them there will reduce the risk of inadvertently using outdated versions. The same applies to this policy. Information should always be checked for accuracy before it is published or used.'*

New text: *'Modern technology makes it easier to access up-to date information and less necessary to keep a local copy of it. For example, it will almost never be necessary to keep a paper copy of a document that is available online. Information should always be checked for accuracy before it is published or used.'*

Reason for change: The council increasingly works in a paperless environment. The encouragement to not store paper copies of online documents applies generally, not just to statutory instruments and government circulars.

Paragraph 4.4 (commentary on the eighth principle)

Old text: *'Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. You should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.'*

New text: *'You should be particularly aware of this when publishing information on the Internet and when using data processing services or cloud-based storage, whose servers may be outside the EEA.*

The European Economic Area (EEA) is the EU Member States together with Iceland, Liechtenstein and Norway.

The European Commission has formally decided that the EU-US Privacy Shield provides an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This means the council can transfer data to an organisation in the United States if the organisation receiving the data is certified under the EU-US Privacy Shield'.

Reason for change: The investigation into the data breach associated with the consultation on public spaces protection orders noted that the commentary on the eighth data protection principle was more restrictive than the requirements of the principle itself, in that the commentary did not provide for processing of personal data outside the EEA in circumstances where there was an adequate level of protection. The new wording rectifies this and makes specific reference to the EU-US Privacy Shield.

Paragraph 4.8

Old text: *'You must make sure that any personal data (on others) which you deal with is kept securely and is not disclosed to any unauthorised third party (see the section on Disclosure of Data for more detail).'*

New text: *'You must make sure that any personal data which you deal with is kept securely and is not disclosed to any unauthorised third party (see the section on Disclosure of Data for more detail).'*

Reason for change: The removed wording in brackets is superfluous as personal data held by the council is always about others.

Paragraph 4.9

Old text: *'All personal data should be accessible only to those who need to use it. You should form a judgement based upon the nature of the information in question, but always consider keeping personal data:*

- *in a lockable room with controlled access, or*
- *in a locked drawer or filing cabinet, or*
- *if computerised, password protected, or*
- *on disks which are themselves kept securely.'*

New text: *'All personal data should be accessible only to those who need to use it. You should form a judgement based upon the nature of the information in question, but always consider keeping personal data:*

- *in a lockable room with controlled access, or*
- *in a locked drawer or filing cabinet, or*
- *if computerised, password protected, or*
- *on removable media which are themselves kept securely.'*

Reason for change: To update the outdated reference to disks in the fourth bullet point to cover other removable media.

5. The EU General Data Protection Regulation is due to come into force on 25 May 2018. The Data Assurance Policy will need to be further revised in due course to take the Regulation into account.

IMPLICATIONS	
Finance	There are no financial implications arising from this report
Legal	Contained in the report
Community Safety	None
Human Rights and Equalities	The Data Protection Act is an important element in the protection of personal privacy.
Sustainability and Environmental Impact	None
Health & Safety and Risk Management	The policy will help the council to comply with its obligations and prove that it complies with them.

LEAD AUTHOR	CONTACT DETAILS	DATE
Ian Curtis	01253 658506	18 May 2017

BACKGROUND PAPERS		
Name of document	Date	Where available for inspection
Data Assurance Policy	November 2014	Town Hall, Lytham St Annes
Data Assurance policy (draft update)		Town Hall, Lytham St Annes
Data Security Breach: Report and Recommendations	31 March 2017	Town Hall, Lytham St Annes or www.fylde.gov.uk/resident/consultation-public-space-protection-order-pspo-do/

Attached documents
1. Data Assurance policy (draft update)