Public Document Pack

Agenda

Delegated Decisions - Cabinet Member for Community & Resources

Date: Tuesday, 4 September 2018

Time: Not required

Venue: Not required

To: Councillor D Mayer

Item		Wards Affected
1	General Data Protection Regulations (GDPR) - Data Protection Officer (DPO) Role *(Pages 3 - 8)*	

Contact: Anne Jenkins, Governance Team Leader
Tel: 01633 656656
E-mail: Cabinet@newport.gov.uk
Date of Issue: 24 August 2017

This page is intentionally left blank

Report

Cabinet Member for Community and Resources

Part 1

Date: 3 September 2018

Subject **General Data Protection Regulations (GDPR) – Data Protection Officer (DPO) Role**

Purpose To seek Cabinet Member approval for the designation of the role of Data Protection Officer (DPO) as a requirement of the post of Digital Services Manager.

Author Rhys Cornwall, Head of People and Business Change

Ward All

Summary Article 37 of General Data Protection Regulation requires Newport City Council to create the role of Data Protection Officer. There is guidance within the Regulations on this role, much of which can be interpreted in a number of ways. The role of Data Protection Officer can be included within other job functions and does not have to be a stand-alone position. Within the report we have assessed the merits and disadvantages of including this role within a number of current positions.

This report seeks approval from the Cabinet Member regarding the designation of the role, with all other decisions relating to staff impacted upon by this the responsibility of the Head of People and Business Change.

Proposal To approve arrangements for the deployment of the designation

Action by Head of People and Business Change

Timetable Immediate

This report was prepared after consultation with:

- Chief Executive
- Strategic Directors
- Head of Law and Standards
- Head of Finance
- Digital Services Manager

Please list here those officers and members you have consulted on this report.

Signed

Background

Article 37 of General Data Protection Regulation requires that organisations meeting certain criteria need a role of Data Protection Officer (DPO). The role of Data Protection Officer is defined in Article 38 of GDPR and this has been summarised by the Information Commissioner's Office (ICO) as below.

- *The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority, or if you carry out certain types of processing activities.*
- *DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.*
- *The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.*
- *A DPO can be an existing employee or externally appointed.*
- *In some cases several organisations can appoint a single DPO between them.*
- *DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.*

The information above states principles but does not specify positions that are appropriate or not appropriate. The Article 29 Data Protection Working Party document 'guidelines on DPO's' provides further interpretation and guidance as below:-

The other tasks and duties of a DPO must not result in a conflict of interests. This means, first, that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case. As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

Independence of the DPO role is a key consideration together with the other requirements of the role. A range of options for the designation of this role are included below, with the preferred option specified. Following Cabinet Member approval the Head of Service will be responsible for undertaking any HR related actions with affected staff.

Financial Summary

- There are no financial considerations as part of this report

	Year 1 (Current) £	**Year 2 £**	**Year 3 £**	**Ongoing £**	**Notes including budgets heads affected**
Costs (Income)					
Net Costs (Savings)					
Net Impact on Budget					

Risks

Risk	Impact of Risk if it occurs* (H/M/L)	Probability of risk occurring (H/M/L)	What is the Council doing or what has it done to avoid the risk or reduce its effect	Who is responsible for dealing with the risk?
Failure to approve the designation of the DPO	M	L	Role will be designated following policy decision by Cabinet Member	Head of People and Business Change

* Taking account of proposed mitigation measures

Links to Council Policies and Priorities
Designation of the role of DPO is a requirement of the General Data Protection Regulation. However, the secure handling, storage and use of data supports the delivery of many council services and therefore links to:

1. Corporate Plan 2017-22
2. Well-being Plan 2018-22
3. Service Area Plans 2018-22

The Council's information risk management framework sets out the Council's approach to information risk management including roles and responsibilities and will be updated to reflect these requirements.

Options Available and considered
All options have advantages and disadvantages and these are detailed following each option. These options have been considered whilst being mindful of the sustainability principles within the Well-being of Future Generations Act.

Option 1: Head of Law and Regulation
The Head of Law and Regulation is the existing Senior Information Risk Owner and has independence from the operational management of the Information Governance function that is line managed by the Head of People and Business Change.

Advantages	**Disadvantages**
Reports to Senior Leadership Team for the organisation	Potential conflict of interests given seniority of role and Regulation function specifically
Knowledge of Data Protection and other legislation	No day to day management of information governance function

Option 2: Head of People and Business Change
The Head of People and Business Change is responsible for the Information Governance function as well as HR, IT etc.

Advantages	**Disadvantages**
Reports to Corporate Management Team	Potential conflict of interests given seniority of role and HR/IT functions specifically
Day to day management of information governance function	Less detailed Data Protection knowledge given the role

Option3: Digital Services Manager
The Digital Services Manager is responsible for the Information Governance function reporting to the Head of People and Business Change.

Advantages	Disadvantages
Access to Corporate Management Team via Head of People and Business Change	No direct access to Corporate Management Team
Day to day management of information governance function	Some small potential for conflict of interests given IT role
Knowledge of Data Protection and other legislation	

Option 4: Information Management Team Leader
The Information Management Team Leader role reports to the Digital Services Manager and is responsible for the Information Governance function.

Advantages	Disadvantages
Day to day management of information governance function	Lower level post more distant from senior management and no direct access to Corporate Management Team so may be deemed inappropriate for the role
Knowledge of Data Protection and other legislation	

Preferred Option and Why
All of the options have advantages and disadvantages with a key issue of independence as against seniority within the organisation. The Digital Services Manager role appears to be the best option given the post's relative seniority, its day to day management of the information governance functions and its knowledge of Data Protection Legislation. **Therefore option 3 is the preferred option.**

Comments of Chief Financial Officer
The proposal to designate the Data Protection Officer responsibilities to the Digital Services Manager has no financial impact. Duties and responsibility will be allocated without any change to pay scales and therefore within existing budget.

Comments of Monitoring Officer
The proposed action is in accordance with the Council's statutory duty under the GDPR to formally appoint or designate an officer as Data Protection Officer, with personal responsibility for monitoring compliance with, and advising the Council on, its data protection obligations. In accordance with Article 37 of the GDPR and the ICO Guidance, the designated post-holder must have sufficient knowledge and expertise in relation to data protection and must also have sufficient independence of operational management of the Council's IT and data processing functions, to avoid any potential conflict of interest. It is, therefore, recommended that the Digital Services Manager post should be formally designated as the Council's DPO. Because the role carries personal responsibility and accountability, the DSM should have direct reporting rights to the Strategic Leadership Team in relation to data protection issues, in order to ensure access to senior management within the Council and to maintain independence (as with the Chief internal Auditor).

Comments of Head of People and Business Change
Designating the role as described within the preferred option will ensure we are compliant with the new regulations (Article 37) and ICO guidance. As author of the report all further comments are contained within the report content.

Comments of Cabinet Member
The Cabinet Member has been briefed on the report and proposals and has approved the content of the report.

Local issues
N/A

Scrutiny Committees

Scrutiny will have opportunity to comment on the deployment as part of the review of the Annual Information Governance Report.

Equalities Impact Assessment and the Equalities Act 2010

The Equality Act 2010 contains a Public Sector Equality Duty which came into force on 06 April 2011. The Act identifies a number of 'protected characteristics', namely age; disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; sexual orientation; marriage and civil partnership. The new single duty aims to integrate consideration of equality and good relations into the regular business of public authorities. Compliance with the duty is a legal obligation and is intended to result in better informed decision-making and policy development and services that are more effective for users. In exercising its functions, the Council must have due regard to the need to: eliminate unlawful discrimination, harassment, victimisation and other conduct that is prohibited by the Act; advance equality of opportunity between persons who share a protected characteristic and those who do not; and foster good relations between persons who share a protected characteristic and those who do not. The Act is not overly prescriptive about the approach a public authority should take to ensure due regard, although it does set out that due regard to advancing equality involves: removing or minimising disadvantages suffered by people due to their protected characteristics; taking steps to meet the needs of people from protected groups where these differ from the need of other people; and encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Children and Families (Wales) Measure

Although no targeted consultation takes place specifically aimed at children and young people, consultation on planning applications and appeals is open to all of our citizens regardless of their age. Depending on the scale of the proposed development, applications are publicised via letters to neighbouring occupiers, site notices, press notices and/or social media. People replying to consultations are not required to provide their age or any other personal data, and therefore this data is not held or recorded in any way, and responses are not separated out by age.

Wellbeing of Future Generations (Wales) Act 2015

The current information risk management framework has not specifically incorporated the five ways of working as a core approach but the report addresses:

- Long term – organisationally this is a long term development with increased maturity of information risk management
- Prevention – preventative measures are key to information risk management especially around staff awareness
- Integration – managing information risk is part of the council's wider risk management process
- Collaboration – information risk is managed in conjunction with the council's IT service delivery partner, the Shared Resource Service (SRS) as well as with suppliers who process data on behalf of the council
- Involvement – the council has direct contact with members of the public and businesses in relation to handling information although this is somewhat reactive.

Crime and Disorder Act 1998

Section 17(1) of the Crime and Disorder Act 1998 imposes a duty on the Local Authority to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent, crime and disorder in its area.

Consultation

N/A

Background Papers

N/A

Dated: 3 September 2018

This page is intentionally left blank