Public Document Pack

Agenda

Delegated Decisions - Cabinet Member for Community and Resources

Date: Tuesday, 11 June 2019

To: Councillor D Mayer

Item		Wards Affected
1	Data Protection Policy *(Pages 3 - 14)*	All Wards

Contact: Anne Jenkins, Governance Team Leader
Tel: 01633 656656
E-mail: Cabinet@newport.gov.uk
Date of Issue: 3 June 2019

This page is intentionally left blank

Report

Cabinet Member for Community and Resources

Part 1

Date: 11 June 2019

Subject **Data Protection Policy**

Purpose To provide a policy for all staff members in relation to Data Protection

Author Information Manager

Ward General

Summary On Friday, 25 May 2018, the European General Data Protection Regulation ('GDPR') came into effect. The Data Protection Act 2018 (DPA 2018), derived from GDPR, describes how organisations must collect, handle and store personal information. Accordingly, a Data Protection Policy has been developed in line with this legislation. The policy offers staff advice and guidance on the practical actions they can take as individuals to comply with the legislation. This report requests the approval of the new policy below.

Proposal **To approve the implementation of the Council Data Protection Policy.**

Action by Information Manager
Head of People and Business Change

Timetable Immediate

This report was prepared after consultation with:

- Head of Law and Regulation – Monitoring Officer, and Senior Information Risk Owner (SIRO)
- Head of Finance – Chief Financial Officer
- Head of People and Business Change
- Information Governance Group
- Data Protection Group

Signed

Background

The Data Protection Act 2018 introduces new obligations on the part of Data Controllers and Data Processors and enhances individual rights regarding data protection. The most significant changes are summarised below.

Data Protection Principles: A new set of Data Protection Principles has been defined and includes an over-arching 'accountability principle' that requires Data Controllers such as the Council to evidence their compliance in detail.

Special Category Data: Special Category Data requires enhanced protections and certain conditions for processing.

Roles and responsibilities: The Data Protection Officer is a new statutory role under the terms of GDPR. The role of Data Protection Officer has been formerly assigned to the Digital Services Manager. To ensure that best practice regarding data protection is implemented consistently across the Council, the Data Protection Working Group meet quarterly to discuss data protection issues. Group membership consists of representatives from each of the service areas.

Rights of individuals: Individual data subjects have new and enhanced rights under the DPA 2018. Individuals have the right to request:

- to access the information that is held about them
- to have their data rectified if it is inaccurate or incomplete;
- to have their data erased;
- to restrict the processing of their data;
- to exercise their right to data portability;
- to object to the processing for the purposes of direct marketing, profiling and automated decision making.

Subject Access Requests: By far the most common individual request received by the council is the right of access to information that we hold about them. This policy seeks to standardise the process across the authority and provide advice and guidance to staff members who receive these requests.

Data Protection by Design and Default: In line with guidance the Information Commissioner (ICO), the new Policy recognises the importance of integrating data protection into the Council's business processes from the start. It includes the use of Data Protection Impact Assessments (DPIAs) as a standard element where use of personal information is proposed and particularly prior to the start of any new projects/technology implementations.

Data Breaches: The Policy recognises the need to report data breaches quickly and effectively to the Information Management team. The policy sign posts staff to the 'incident reporting policy' and offers guidance to staff in the event that they are unsure if a breach has occurred.

Accountability: The policy seeks to communicate the importance of data protection and ensure that staff are aware of their responsibilities in relation to data sharing, disposal of personal information and the creation of effective privacy notices where appropriate.

Financial Summary

There are no financial implications to this report.

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 implement a Data Protection Policy within the Council could mean facing a significant financial penalty if it acts in breach of the new rules. Many data protection breaches are caused by human error (e.g. sending an email to the wrong person for example) and can be difficult to eradicate. However, the Council will need to continue to take action to minimise the risk of data protection breaches and to ensure DPA 2018 compliance. This will include, for example, the provision of staff training and the development of new policies such as this one.	H	M	The data protection policy provides clear advice and guidance to staff in relation to the process of reporting any data breaches or suspected data breaches in a timely manner. The policy references data protection training for staff and how to book onto this training.	Information Manager
Failure to comply with individual rights in respect of data protection requests may result in the authority being reported to the Information Commissioners Office (ICO) and may lead to further regulatory action.	M	L	The data protection policy seeks to standardise the process to comply with individual data requests across the authority. The policy provides clear advice and guidance to staff.	Information Manager

* Taking account of proposed mitigation measures

Links to Council Policies and Priorities

There is no direct link to meeting the Council's Priorities. However, the implications of the drive of being Digital by Design and Smart Working across the Council will increase the focus on protecting personal data. The Data Protection Policy will underpin this requirement. As a result of the Council applying the Data Protection Policy, residents of Newport can be assured that any personal data held by the Council will be used only for the purpose it is intended.

Options Available and considered

1) Do nothing.
2) Implement the corporate Data Protection Policy.

Preferred Option and Why

2) Implement the corporate Data Protection Policy – It is vital that the organisation complies with the Data Protection Act 2018. This policy provides staff with the appropriate advice, guidance and support to ensure that information is appropriately and securely managed throughout the organisation.

Comments of Chief Financial Officer
There are no direct financial implications as a result of approving this policy but the Council would be at risk of incurring significant financial penalties if no policy is in place. Any actions required to adhere to the policy once in place will be met from existing budgets.

Comments of Monitoring Officer
The proposed Data Protection Policy is consistent with the Councils' legal obligations under the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) in relation to the collection, processing and storage of personal data, both electronically and manually. The policy provides appropriate practical advice and guidance to both staff and elected members to ensure compliance with the legislation.

Comments of Head of People and Business Change
As author of the report, the comments of the Head of People and Business Change are contained within the body of the report.

In particular, the Data Protection Policy seeks to communicate the importance of data protection and ensure that staff are aware of their responsibilities in relation to data sharing, disposal of personal information and the creation of effective privacy notices where appropriate. A key aim is that everyone processing personal information understands their responsibilities and receives appropriate information to support them, including the relevant "information security" training.

The Data Protection Officer is a new statutory role under the terms of GDPR. In NCC: the role of Data Protection Officer has been formerly assigned to the Digital Services Manager and there are therefore no new staffing requirements associated with this report.

The proposal is in accordance with the sustainable development principle in the Well-being of Future Generations Act.

Comments of Cabinet Member
I support the need for Newport City Council to implement a Data Protection Policy. Good data protection and information security practice is vital to ensure information is appropriately and securely managed throughout the organisation. The policy outlines the importance of complying with the Data Protection Act 2018 and the need to make all staff members aware of their own responsibility and that of their service.

Local issues
None identified

Scrutiny Committees

Equalities Impact Assessment and the Equalities Act 2010
There are no equalities implications of this report and so there is no requirement for a Fairness and Equalities Impact Assessment to be completed for this report.

Children and Families (Wales) Measure

Wellbeing of Future Generations (Wales) Act 2015
Information governance is a key part of the Council's corporate governance arrangements and is reflected in the Corporate Risk Register.

Effective governance of the Council's information underpins all Council activities, safeguarding information assets and using them to maximum effect to help achieve the Council's Priorities and Wellbeing Objectives, as well as the Well-being Goals of the Future Generations Act (Wales) 2015.

This report contributes to the Well-being Goals and is consistent with the five ways of working as defined within the sustainable development principle in the Act in that effective management of the Council's information will ensure reliable, high quality information is held which could be shared with other partners to ensure a joined up approach to providing services and preventing problems, as well as to enable close working with communities affected by the Council's activities.

A primary aim of the policy is to prevent data breaches and mishandling of personal information by the Council.

Integrating data protection into the Council's business processes is a key element of this proposal: through Data Protection Impact Assessments (DPIAs) as a standard element where use of personal information is proposed and prior to the start of any new projects/technology implementations.

Reliable information also ensures that decisions are more robust now and in the long-term and preservation of the Council's historic record means that current and future generations can hold the Council to account for its decisions and learn from previous activities.

Crime and Disorder Act 1998

No issues identified.

Consultation

No specific further consultation.

Background Papers

Dated: 11 June 2019

Data Protection Policy

Created by	Jodi Pontin
Date	2019
Reviewed by	Tariq Slaoui
Date	05/02/2019

Document Control

Version	Date	Author	Notes / changes
V0.1	05/02/19	Jodi Pontin	1st draft
V0.2	20/02/19	Tariq Slaoui	Reviewed
V0.3	18/04/19	Tariq Slaoui	Reviewed

Contents

Golden Rules

The following are the key rules that must be followed when using the policy; these points do not replace the full policy, which you should also familiarise yourself with.

The Data Protection Act 2018 is not a barrier to sharing information but ensures personal information is shared appropriately

The DPA 2018 gives individuals certain rights. One of those rights is the right to access all of the data that we hold about them. This is called a **Subject Access Request**, If you receive such a request, please contact the Information Management team.

Any breaches of personal data should be reported to the Information Management Team immediately, as per the Information Security Incident Reporting Policy. If you are unsure then please contact Information Management for advice.

It is the Councils responsibility to be open, honest and transparent with individuals as to how, why and with whom their data is being processed. Our Privacy Notices explain how and why we process personal information.

All staff have a part to play and are accountable in the compliance of GDPR

If in doubt seek advice. For further guidance, contact the information management team information.management@newport.gov.uk

1. Introduction

1.1 Newport City Council handles and stores a large amount of data across the organisation to carry out duties as a local authority. The Data Protection Act 2018 (DPA 2018) and the EU General Data Protection Regulation (GDPR) describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically or on paper.

1.2 The purpose of this policy is to describe Newport City Councils approach to Data Protection in line with the Data Protection Act 2018. Newport City Council is committed to protecting the integrity and confidentiality of personal data by using the appropriate technical or organisational measures to ensure its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

1.3 The Data Protection Act 2018 is under pinned by six important principles. These principles state that data must be:

- Processed fairly, lawfully and transparently
- Collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they were collected
- Accurate and, where necessary, kept up to date.
- Kept no longer than is necessary
- Handled and processed securely

2. Scope and definitions

2.1 This policy covers Newport City Councils obligations under the Data Protection Act 2018.

2.2 This policy applies to all Council employees, elected members and individuals/partners working on behalf of Newport City Council who have access to personal information that the Council has responsibility for.

2.3 This policy covers all data that Newport City Council holds in relation to identifiable individuals.

2.4 'Personal Data' means any information relating to an identified or identifiable living person (data subject). An identifiable person is one who can be identified by reference to an identifier such as a name, reference number, location etc.

2.5 'Special Categories' of data require further protection. This covers the following:

- Racial or ethnic origin;
- Political opinions;
- Philosophical beliefs;
- Trade Union membership;
- Genetic data;
- Biometric data;
- Health data;
- and sex life or sexual orientation

3. Individuals Rights

3.1 The Data Protection Act 2018 gives individuals a number of rights. Please note that not all of these rights are absolute and the organisation will need to consider the request upon receipt.

Individuals have the right to request:

- to access the information that is held about them
- to have their data rectified if it is inaccurate or incomplete;
- to have their data erased;
- to restrict the processing of their data;
- to exercise their right to data portability;
- to object to the processing for the purposes of direct marketing, profiling and automated decision making.

In all instances, the request needs to be addressed to:
information.management@newport.gov.uk

3.2 The right to be informed. All individuals are entitled to have access to data that the organisation holds on them. This is known as a **Subject Access Request.**

3.1 **Subject Access Requests** can be received in writing or verbally. The request should be clearly stated and specific in order for the response to be accurate and delivered within the designated timescale. **If you receive a request for information, it is important that you pass the details on to the information management team straight away.**

3.2 It is requirement to verify the identity of the requester and, in the case of information for a child under the age of 13; proof of parental responsibility or legal guardianship. For a request made on someone else's behalf, signed consent will be required.

3.3 Information should be provided to the requester via a secure mechanism. If sending electronically, Egress should be used. Where this is not possible, the requester can collect the information in person. Subject Access Requests should not be sent via post as there is an increased risk of loss of data. Guidance should be obtained from the information management team in the event that neither option is practicable.

3.4 Requests are to be responded to within one month, this is calculated from the date of receipt of all identification and relevant documentation. Due to an increase in the number and complexity of requests the authority has committed to responding to at least 75% of requests within one month.

4. Compliance

4.1 Any breaches of personal data should be reported to the Information Management Team, immediately, as per the Information Security Incident Reporting Policy. If you are unsure then please contact Information Management for advice.

4.2 Serious data breaches will be considered by the Senior Information Risk Owner, following the advice of the Data Protection Officer and consideration will be given to informing the Information Commissioner's Office (ICO).

4.3 Failure to comply with the law on Data Protection may result in:

- Serious consequences for individuals that the data relates to, including embarrassment, distress, financial loss
- Irreparable damage to the Council's reputation and loss of confidence in the Council's ability to manage information properly
- Monetary penalties and compensation claims
- Enforcement action from the Information Commissioner

- Personal accountability for certain criminal offences

4.4 Newport City Council seeks to minimise the risk of non-compliance with appropriate technical and non-technical security measures, policies, procedures and training.

4.5 The Information Management team offer 'Information security' training for staff. This is bookable via the employee Learning & Development Directory here

5. Accountability

5.1 Newport City Council shall be responsible for, and be able to demonstrate compliance with the Data Protection Act 2018.

5.2 The authority has a statutory duty to appoint a Data Protection Officer (DPO). The designated DPO for Newport City Council is:

Digital Services Manager
Email: information.management@newport.gov.uk
Tel: 01633 656656

5.3 Heads of Service, as Information Asset Owners, adhere to the Council's Information Risk Management Policy

5.4 Data Protection Impact Assessments will be undertaken at an early stage whenever use of personal information is proposed and particularly prior to the start of any new projects.

5.5 Clear privacy notices are communicated and easily available. These enable individuals to understand how their personal information is being used. Privacy notices are published at www.newport.gov.uk/privacynotice

5.6 The sharing of personal information is carried out in compliance with approved protocols, such as the Wales Accord on Sharing Personal Information and data processor agreements.

5.7 Disposal of personal information is in line with the Council's Information Retention and Disposal Policy.

5.8 Everyone processing personal information understands their responsibilities and receives appropriate information to support them, including the relevant training

6. Complaints

6.1 If an individual is unhappy with the way Newport City Council is using their data, they have the right to make a complaint.

This can be done by sending an email to information.management@newport.gov.uk stating the full details of the complaint.

6.2 If the individual is not content with the outcome of their complaint, they may apply directly to the Information Commissioner for a decision.

Generally, the Information Commissioner's Office (ICO) cannot make a decision unless council's complaints procedure has been exhausted.

The Information Commissioner can be contacted at:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF

7. Related Policies and Resources

7.1 This policy should be read in conjunction with the following Council policies and guidance:

GDPR Privacy Notice
Information Risk Management Policy
Incident Reporting Policy
Information Security Incident Reporting Form
Information Sharing Policy
Information Retention and Disposal Policy
Access to Network, Email and Internet Policy
Agile Working Policy

8. Further Information

8.1 Further advice and guidance is available from the Information Management Team:

Information.management@newport.gov.uk

This page is intentionally left blank