NEWTOWN AND LLANLLWCHAIARN TOWN COUNCIL

DATA PROTECTION POLICY*

1 Introduction

In complying with the Data Protection Act 2018 the Town Council shall ensure that all data is**:

- Processed fairly, lawfully and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational features
- Where the lawful basis for processing data is consent, the Town Council shall ensure that consent is freely given, unconditional and explicit.
- The Town Clerk shall take any reasonable necessary steps to ensure the security of council data; this shall include ensuring that access to data is limited and that data is disposed of securely.
- The Town Council does not use automated decision making or profiling of individual personal data.
- The Town Council shall ensure that any third party which processes data on its behalf has sufficient data protection, security measures and breach reporting procedures in place and this shall form part of the terms and conditions of any contract entered into.
- Data related to a child (under 13) will not be processed without the express parental/guardian consent of the child concerned

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

- Members and employees must abide by any procedures developed in accordance with this policy and failure to do may result in disciplinary proceedings or suspension of access to council resources.

- The Town Clerk shall ensure that a Data Audit is undertaken at least annually.

- Any data transferred outside the European Economic Area (EEA) will only be places on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union.

  **A glossary of common terms used is help in Appendix 1

2 Training & Guidance

2.1 All members and employees of the council shall receive an induction on Data Protection and training as required.

2.2 The Town Clerk shall ensure guidance notes on Data Protection for both members and employees to provide easy to access guidance on Data Protection practices. (See the 8 Briefing Notes for staff & councillors)

3. Privacy Notices

3.1 The Town Clerk shall ensure the production of Privacy Notices as required which will be published on the Town Council website. They shall be reviewed at least annually. Privacy Notices may vary depending on the data being collected/held.

3.2 The Town Council will use a blended approach to provide privacy information to individuals; providing information at the point of collection and reference to the full Privacy Notice where it is not practical to provide the notice in full at the point of collection.

3.3 At collection sufficient information will be given to detail why the data is being collected, how it will be used, how long it will be kept for and whether it will be shared with any third party.

3.4 Privacy Notices will be prepared with reference to guidance from the Information Commissioner's Office and shall be provided in simple language in a clear font.

4 Breach Reporting

4.1 A data breach is defined as a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'

4.2 The Town Clerk shall ensure procedures are maintained to safeguard against potential data breaches. See Appendix 2 attached.

4.3 All data breaches shall be reported to the Town Clerk who shall maintain a record of data breaches and determine, in accordance with Information Commissioner's Office guidance whether the breach must be notified.

5 Data Protection Impact Assessments

5.1 A Data Protection Impact Assessment is a process to identify and minimize the data protection risks of a project. It is mandatory for certain types of data processing or processing which is likely to result in a high risk to individuals' interests.

5.2 The Town Clerk shall ensure procedures for determining if a DIPA is required and the undertaking of the same. See Appendix 3 attached.

6 Data Retention

6.1 The Town Council will only keep data for as long as it is necessary to do so.

6.2 The council's standard data retention requirements are detailed in the Retention, Disposal and Archiving of Records Policy.

7 Data Subject Rights

7.1 A data subject has the right to:

- Access their information
- Correct information held which they believe is incorrect
- Request information is deleted
- Object to the processing of data
- Request data is transferred to another data controller
- Withdraw consent for processing of data
- Lodge a complaint with the Information Commissioner's Office

7.2 A data subject wishing to exercise their rights may do so by contacting the Town Clerk.

Contact : Ed Humphreys – Town Clerk
Email townclerk@newtown.org.uk
Telephone 01686625544
Address

See Appendix 4 attached.

8 Review and Monitoring

8.1 This policy shall be reviewed periodically and in light of experience, comments from data subjects and guidance from the Information Commissioners Office.

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

The Finance & General Purposes Committee adopted this Policy for Data Protection at its meeting on

……9/3/15…….

Review Date = every 2 years

Amended or Reviewed	Date	Version No	Who
Approved	9/3/15	090315a/1	Phil Watkins
Reviewed	26/9/16	090315a/1	Richard Edwards -Mayor
Reviewed	25/9/17	090315a/1	Sue Newham - Mayor
Reviewed & Amended	26/11/18	090315a/2	Sue Newham - Mayor

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

Appendix 1 – Glossary of Terms

Data subject - means the person whose personal data is being processed. That may be an employee, prospective employee, associate or prospective associate of BTC or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.
It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.
Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Town Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

Appendix 2 – Process to guard against data breaches

A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

There is an obligation to notify certain breaches to the ICO within 72hours and may need to notify some data subjects.

The procedures to detect, investigate and report a breach are contained in the Data Protection Log – maintained by the Town Clerk.

A Compliance Log will also be maintained to demonstrate the appropriate security, technical and organisational measures are being maintained.

Examples of personal data breaches and steps to avoid them (organisational measures)

Example	**Measure**
Emails and attachments being sent to the wrong person or several people.	Slow down! Check thoroughly before clicking send.
The wrong people being copied in to emails and attachments.	Use BCC (Blind Carbon Copy) where necessary.
Lost memory Sticks which contain unencrypted personal data	Adopt a protocol for memory sticks.
Malware (IT) attached.	Ensure up to date anti-virus is in place
Equipment theft.	Check security provisions.
Loss of personal data which is unencrypted	When necessary encrypt personal data

All new projects and services where a project initiation document is initiated will incorporate 'privacy by design' to ensure data protection is considered.

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

Appendix 3 - Data Protection Impact Assessments

Data Protection Impact Assessments (DPIA) should be carried out when

- new technology is deployed
- where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale .

If two or more of the following apply, it is likely that the Council will be required to carry out a DPIA. This does not apply to existing systems but would apply if we introduce a new system.

1.	Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests.	□
2.	Automated-decision making. Example: when processing leads to the potential exclusion of individuals.	□
3.	CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects.	□
4.	Sensitive personal data as well as personal data relating to criminal convictions or offences.	□
5.	Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed.	□
6.	Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. you merge your mailing list with another council, club or association.	□
7.	Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients.	□
8.	"New technologies are in use". E.g. use of social media, etc.	□
9.	Data transfers outside of the EEA.	□
10.	"Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking.	□

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

If 2 or more of the above are ticked it is mandatory that a DPIA is carried out.

The following checklist helps us make an assessment and issues to be considered in more detail for our DPIA

a) What is the objective/intended outcome of the project?

b) Is it a significant piece of work affecting how services/operations are currently provided?
c) Who is the audience or who will be affected by the project?
d) Will the project involve the collection of new personal data about people? e.g. new identifiers or behavioural information relating to individuals
e) Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?
f) Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?
g) Is data being processed on a large scale?
h) Will the project compel individuals to provide personal data about themselves?
i) Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?
j) Will personal data be transferred outside the EEA?
k) Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?
l) Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?
m) Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)
n) Is monitoring or tracking or profiling of individuals taking place?
o) Is data being used for automated decision making with legal or similar significant effect?
p) Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)
q) Is sensitive data being collected including:

    (i) Race

    (ii) Ethnic origin

    (iii) Political opinions

(iv) Religious or philosophical beliefs

(v) Trade union membership

(vi) Genetic data

(vii) Biometric data (e.g. facial recognition, finger print data)

(viii) Health data

(ix) Data about sex life or sexual orientation?

r) Will the processing itself prevent data subjects from exercising a right or using a service or contract?

s) Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?

t) Will the project require contact to be made with individuals in ways they may find intrusive?

When two boxes are ticked the following paperwork will be fill in:

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

Newtown & Llanllwchaiarn Town Council

Data Protection Impact Assessment

Who is considering DPIA?		
Name	Job Title	Email address
Project Summary		
Project Name		
Parties Involved		
Date		
Identify Need for DPIA		
Purpose of Project Benefits to NLTC Benefits to individuals		
Why was the need identified? What personal data is in the project		
Describe the personal information/personal data flows		
Information Flows – collection, use, transfer & deletion of personal data		

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk

Does any data processing involve: • High Risk to individuals rights • Systematic evaluation of personal data – profiling • Large Scale processing of sensitive information • Large scale surveillance of public areas	
Assess project against Key Data Protection Principals	
(i) Lawfulness, Fairness and Transparency	a) What categories of personal data are being collected? Any special categories? b) Where do you obtain the personal information form? c) What information is provided to the individual? What Privacy Notice applies? d) How will you make the processing lawful? (pick one) o Consent? (How are you doing this – was it freely given? specific, informed and unambiguous). How will it be recorded? o Contract performance to collect and process data o Compliance with legislation? o Necessary for the performance of a task carried out in the public interest? o Legitimate interest – (public authorities cannot use this one)
(ii) Purpose Limitation	a) For what purpose do you wish to use the personal data collected? b) How will you notify individuals of these purposes? c) How will you ensure the data are not further processed for incompatible purposes?

(iii) Data Minimisation	a) Are all the data collected necessary for the purposes for which they are processed? b) What steps are you taking to ensure you only collect the minimum personal data you need for the purposes of the project?
(iv) Accuracy	a) If you are procuring new software does it allow you to amend and update the data where necessary b) How will you ensure that the personal data collected are accurate e.g.use reliable source c) How will you verify the accuracy of the data, and how often? d) How will you erase or correct personal data promptly, if there are errors?
(v) Storage Limitation	a) What retention periods are suitable for the personal data you are collecting? b) If you plan to anonymise data, so that individuals can no longer be identified, please explain how and when?
(vi) Rights of Individuals	a) Will the project systems allow you easily to provide, amend or delete information on request, or restrict the processing of information b) Where processing is based on consent or contract necessity, and automated, will the project systems all you easily to provide personal data to and individual? c) Where processing is based on consent, will the project systems enable the individual to withdraw that consent as easy as it was given? d) Will any decisions that affect individuals be made solely on the basis of processing automatic means? If so, will the project systems allow the individuals to object to any processing e) If this is a marketing project, can individuals opt-out of their information being used for a purpose(e.g. for profiling in the course of targeted advertising)?

(vii) Security, Integrity and Confidentiality	a) What technical security will be in place e.g. encryption, firewalls, relevant information security policies? b) What organisational security will be in place e.g. secure disposal, staff training, limits on access? How are staff authorised to access the data and how is access restricted?
(viii) International Transfer	a) Will personal data be transferred outside the country in which it is collected? b) If so, what adequate safeguards will be put in place e.g.EU model clauses? c) Has the party to whom the data is being transferred been subject to a due diligence exercise to determine their security and handling of personal data to ensure compliance with NLTC data protection policies?
(ix) Data Processors	a) Will third party process NLTC data? If so, what reasonable steps has NLTC taken to ensure that they comply with data protection requirements? b) How do you assess their data security measures? How do you ensure they comply with these measures? c) Does the contract in place with the third party vendor contain suitable data processor obligations in line with the requirements of Data Protection Laws

Identify Privacy Risks of the Project – referring to the previous step
Identify Solutions to the Privacy Risks

Privacy	Privacy Issue/Risk –	Solution/Action to be	Result – Is the risk	Who will	Who should be	Deadline for

Principal	to individuals, compliance or corporate	taken	eliminated, reduced or accepted	implement	consulted? (ICO?)	implementation
(i)						
(ii)						
(iii)						
(iv)						
(v)						
(vi)						
(vii)						
(viii)						
(ix)						

Evaluation	
Is the final impact on individuals after implementing each solution justified, compliant and proportionate response to the aims of the project?	
Integrate the DPIA outcomes back into project plan	
Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork?	
Name of contact for any privacy concerns that may arise in the future	

Approval			
Name	Position	Signature	Date

Appendix 4 – Data Subject Requests

1. Upon receipt of a subject access request officers will inform the Town Clerk.
2. Identify if the request has been made under the Data Protection legislation.
3. A request will result in an exhaustive search (by officers or councillors) to locate and supply any personal data.
4. All personal data that has been requested must be provided unless and exemption can be applied for.
5. All requests accepted as valid will be replied to within one calendar month.
6. All Subject Access Requests will be undertaken free of charge, unless the legislation permits reasonable fees.
7. All councillors and staff must be made aware and follow this policy and guidance.
8. When a requestor is not satisfied with a response we must manage it as a compliant.

Procedures to follow for compliance

	SAR process	**Actions**
1.	Receive Request	Inform Town Clerk. Add to SAR log
2.	Identify request made under Data Protection legislation	Check request is in writing and defines what they are requesting. They must supply their address and valid evidence to prove their identity.
3.	Search for personal data	A search to be made of such things as: emails, archived emails, emails deleted but recoverable, word documents, spreadsheets, databases, memory sticks, floppy discs, CDs, tape recordings, paper records in filing systems etc.
4.	Provision of data	An explanation should be provided with all personal data supplied. Any codes, acronyms and complex terms should be explained. Information should be proved in a permanent form unless agreed otherwise. Any exempt information should be redacted and explain why it has.
5.	Reply within one calendar month	Make this clear on any forms and our website.
6.	Requests are free unless legislation allows otherwise	Compliance through induction, appraisals and training. Adopt appropriate working practices.
7.	Staff and councillors aware	Maintain a log to allow council to report om the volume of requests and compliance against those requests.
8.	Requestor not satisfied with response	When responding to a compliant the requestor to be advised that they may complain to the ICO if they remain unhappy with the response.

*Mae fersiwn Cymraeg ar gael oddi wrth clerc y dref / A Welsh language version is available upon request from the Town Clerk