PADSTOW TOWN COUNCIL: 24 FEBRUARY 2026

AGENDA ITEM 14: ASSERTION 10 - DATA PROTECTION POLICY AND WEBSITE COMPLIANCE

1. Overview

1.1 Following Council's decision that the Town Clerk undertake the role of Data Protection Compliance the Town Clerk considered it prudent to undertake a complete review of Council's Data Protection Policy. Appendix 1 is for Council consideration which the Town Clerk reviewed taking into account advice from NALC and best practice from other Councils.

1.2 In light of the Town Clerk's compliance role, all General Privacy Notices require amendment to delete reference to the former outside support of a DPO officer and instead replace with the role of Town Clerk as Data Protection Compliance.

1.3 The Town Council has an Accessibility Statement on its website, the Town Clerk is seeking advice as to whether this requires updating from Council's website support, at the time of writing this advice isn't forthcoming. She hopes to provide this further information at the Council meeting.

2. Council Consideration

2.1 Council is asked to i) agree and adopt the Data Protection Policy (appendix 1); ii) all General Privacy Notices be amended as per 1.2 above; and iii) subject to advice from Council's website support its website Accessibility Statement be updated as appropriate.

AGENDA ITEM 15: USE OF COUNCIL LAND - RAILWAY CAR PARK

1. The Council Chair, Vice Chair and Town Clerk will provide update at the meeting as to the meeting and it is expected that revised costs will tabled at the meeting for Council's further consideration.

2. The Town Clerk has also sought advice from Fernbank concerning a heritage style bus stop, as requested by Council to fit better within the surrounds of the Council Office. Appendix 1 to this report shows photos of option suggesting being the Heritage Shelter which can have either a flat (sedum plants) or pitch roof. The photos depicting the pitch roof option. The Town Clerk is seeking clarity on costings and will report this to the Council meeting.

Agenda item 14 - Appendix 1

PADSTOW TOWN COUNCIL

Data Protection Policy

POLICY/PROTOCOL/PROCEDURE			
Version	Draft	**Comments**	
Approval Date		**Responsible Officer**	Town Clerk
Committee	FGP	**Approval by**	Full Council

VERSION HISTORY		
Date	**Version**	**Comments**
18.2.26	Draft	Reviewed current Policy to update and include TC Compliance role as agreed by Council.

REVIEW RECORD		
Date Review initiated	**Review undertaken by i.e. officer/ Cttee/Council**	**Summary of any recommended updates/changes to be made**

Purpose
Padstow Town Council is committed to being transparent about how it collects and uses the personal data of individuals, and to meeting its data protection obligations.

This policy sets out the Council's commitment to data protection, and individual's information rights and obligations in relation to personal data in line with Data Protection Law which includes but may not be limited to the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulation (PECR).

This policy applies to the personal data of any individuals that the Council may need to process in order to meet its objectives including its current and former job applicants, employees, workers, contractors and former employees. For the avoidance of doubt this policy also applies to the personal data relating to members of the public or other personal data processed for Council business.

Who is Responsible for this Policy and its Compliance?
The "Council" is the Data Controller which means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed and as such should ensure that this Policy is in place and adopted.

The Council, as corporate body, had ultimate responsibility for ensuring compliance with the Data Protection legislation. It has appointed the Town Clerk as the person with responsibility for Data Protection Compliance within the Council. Questions about this policy, or requests for further information, should be directed to the Town Clerk.

Definitions
"Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised or statistical data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceeding

Data Protection Principles
The Council processes personal data in accordance with the following data protection principles the council:

- processes personal data lawfully, fairly and in a transparent manner
- collects personal data only for specified, explicit and legitimate purposes
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing

- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

The Council will inform individuals of data it processes, the reasons for processing the personal data, how we use such data, how long we retain the data, and the legal basis for processing in our privacy notices.

The Council will not use personal data for an unrelated purpose without informing the individuals about it and the legal basis that we intend to rely on for processing it. The Council will not process personal data if it does not have a legal basis for processing.

The Council keeps a record of our processing activities in respect of the personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

Processing: Personal Data
The Council will process the personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., your contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

If the Council processes the personal data (excluding special categories of personal data) in line with one of the above bases, it does not require the consent of the individual. Otherwise, the Council is required to gain consent to process the personal data. If the Council asks for consent to process personal data, then it will explain the reason for the request. You do not need to consent or can withdraw consent later.

Sometimes the Council will share the personal data with contractors and agents to carry out its obligations under a contract with the individual or in its legitimate interests. We require individuals or companies to keep such personal data confidential and secure and to protect it in accordance with Data Protection law and the council's policies. They are only permitted to process the data for the lawful purpose for which it has been shared and in accordance with the council's instructions and where they act as a data processor.

Processing: Special Categories of Data
The Council will only process special categories of personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement;

- where it is necessary to protect your vital interests or those of another person where you are physically or legally incapable of giving consent;
- where you have made the data public;
- where it is necessary for the establishment, exercise or defence of legal claims;
- where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity;
- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;
- where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
- where is it necessary for reasons of public interest in the area of public health; and
- where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

If the Council processes special categories of personal data in line with one of the above bases, it does not require the consent of the individual. In other cases, the Council is required to gain consent to process your special categories of personal data. If the Council asks for consent to process a special category of personal data, then it will explain the reason for the request.

Individual Rights
All data subjects for whom the Council may process personal data have a number of rights in relation to your personal data.

Subject Access Requests
Individuals have the right to make a subject access request. If such a request is received, the Council will endeavour to inform the requester:

- whether or not their personal data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- to whom the personal data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- for how long the personal data is stored (or how that period is decided)
- the rights to rectification or erasure of data, or to restrict or object to processing. the right to complain to the Information Commissioner's Office (ICO) if the individual thinks the Council has failed to comply with their data protection rights; and
- whether or not the Council carries out automated decision-making and the logic involved in any such decision-making.

The Council will also provide individuals with access to personal data undergoing processing. This will normally be in electronic form unless otherwise agreed.

If additional requests are made to access the personal data, the Council may charge a fee, which will be based on the administrative cost to the Council of providing the additional copies.

To make a subject access request, the individual should send the request to the Town Clerk. In some cases, the Council may need to ask for proof of identification before the request can be processed. The Council will inform the individual if it

needs to verify the identity of the individual and the documents that may be required.

The Council will normally respond to a request within a period of one month from the date it is received. Where the Council processes large amounts of personal data, this may not be possible within one month. The Council will inform the individual within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. Alternatively, the Council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Council has already responded. If an individual submits a request that is unfounded or excessive, the Council will notify them that this is the case and whether or not it will respond to it.

Other Rights
Individuals have a number of other rights in relation to your personal data. They can require the Council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the council's legitimate grounds for processing data (where the Council relies on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the council's legitimate grounds for processing data.
- complain to the Information Commissioner's Office (ICO). The Council will ensure that individuals are aware they may complain and provide contact details of the ICO in the public domain and upon request.

Data Security
Padstow Town Council cares to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and relevant policies.

We will only keep your data for the purpose it was collected for and only for as long as is necessary, after which it will be deleted or shredded.

Where the Council engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact Assessments
Some of the processing that the Council carries out may result in risks to privacy (such as monitoring of public areas via CCTV). Where processing would result in a high risk to individual's rights and freedoms, the Council will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks to individuals and the measures that can be put in place to mitigate those risks.

Data Breaches
The Council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the Council must take notes and keep evidence of that breach.

If the Council becomes aware of a data breach, details of the incident will be sent to the Town Clerk without delay to ensure appropriate action may be taken. This may include reporting such a breach to the Information Commissioner. Regardless of the severity of the circumstances and potential impact on individuals' rights, the incident will be recorded.

If the Council discovers that there has been a breach of data protection law concerning personal data that poses a serious risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will inform the individuals concerned that there has been a breach and provide them with information about its likely consequences and the mitigation measures the Council has taken.

International Data Transfers
The Council may not transfer HR-related personal data to countries outside the EEA.

Individual Responsibilities
Individuals are responsible for helping the Council keep the personal data up to date. The individual should let the Council know if data provided to the Council changes, for example if they move to a new house or change their bank details. All individuals who may work for, or on behalf of, the Council have some responsibility for ensuring data is collected, stored and handled appropriately and in line with the council's policies.

Such individuals may have access to the personal data of other individuals and of members of the public in the course of their work with the council. Where this is the case, the Council expects such individuals to help it meet the data protection obligations included in this policy. Individuals who have access to personal data are required:

- to access only data that they are authority to access and only for authorised purposes.
- not to disclose data except to individuals (whether inside or outside the council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of the Council
- to ask for help from the council's data protection lead if they are unsure about data protection or if they notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

Training
The Council provides training to all individuals about their data protection responsibilities.

If the individual's roles require them to have regular access to personal data, or they are responsible for implementing this policy or responding to subject access requests under this policy, they will receive additional training to help them understand their duties and how to comply with them.

This is a non-contractual policy and procedure which will be reviewed from time to time.

Cornwall
Air Ambulance
Help us 'Sing it Home' this Christmas
We need you now, more than ever, to help bring your second helicopter home.

HUB

CENTENARY WESLEYAN CHURCH.

CENTENARY