Prestatyn Town Council

General Data Protection Regulation (GDPR)

Policy & Procedures

2025

VERSION UPDATES

Version	Date	Section	Details of change
V1D2	21.12.2023	Whole of document	New document
V2	19.06.2025	Minor changes	Updated

APPROVALS AND DISTRIBUTION

Version	Date	Meeting	Reference
V1			

Contents

COMMITTMENT

PRESTATYN TOWN COUNCIL PROMISES THAT IT WILL:

- Value the personal information entrusted to us and make sure we respect that trust, making sure information is only shared where operationally necessary.
- Go further than just the letter of the law when it comes to handling personal information by adopting and following good practice standards.
- Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems.
- Be open and transparent with individuals about how we use their information and who we give it to.
- Make it straightforward for individuals to access all their personal information.
- Keep personal information to the minimum necessary and delete it when no longer needed.
- Have effective safeguards in place to ensure personal information is kept securely and only shared in line with the current policy and legislation.
- Provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly.
- Put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises.
- Regularly check that we are meeting our obligations and our promises and report on how we are doing.

INTRODUCTION

Whilst the Policies and procedures outlined in this document refers to General Data Protection Regulation (GDPR), Prestatyn Town Council (PTC) shall at all times comply with its duties under United Kingdom legislation regarding data protection. This includes, but is not limited to the below:

- The Data Protection Act 2018 (DPA) incorporating the General Data Protection Regulation (GDPR) legislation that places legal obligations on organisations who collect and use personal information, giving individuals certain rights of access. In addition, there are stricter requirements in the Act in respect of processing 'special category data'.
    - Special category data includes personal data revealing or concerning race, political opinions, religion, health, etc *(see DPA 2018)*. This does not include criminal offence data, which is dealt with separately.
- The rights of privacy and respect for personal and family life, as set out in Article 8 of the Human Rights Act 1998 (HRA).
- The Freedom of Information Act 2000 (FOIA)
- Environmental Information Regulations 2004 (EIRs)

Personal information can be held in any format, for example, electronic, paper records, CCTV or photographic images and the legislation applies irrespective of how the information is held.

PRESTATYN TOWN COUNCIL'S RESPONSIBILITIES UNDER GDPR

PTC (PTC) is committed to ensuring all staff, including elected members, volunteers and contractors comply with UK GDPR.

All staff must undertake PTC's mandatory training on 'Data Protection - Understanding GDPR' as part of their induction. Refresher training must then be completed again each year by all staff. All staff are responsible for ensuring compliance with the Act.

Where a request is received under the Freedom of Information Act (FOIA) or the Environmental Information Regulations 2004, but in fact it falls within the Data Protection regime, PTC will channel it through the appropriate policy (as different exemptions and therefore different legal rights apply in the circumstances). In some circumstances, a request may fall under two or more of these regimes; and in this situation, some information may need to be withheld under one regime but released under the other. The public interest test, applicable to both DPA and FOIA, will be a key component of our decision making, to enable the public and citizens sharing their information or data with us to have confidence that we are delivering our functions to the quality and standard required by law and the communities served by PTC.

PTC's elected members are data controllers in their own right in respect of processing the data that they collect relating to their wards and constituents. When they are processing Council information, PTC remains the responsible party to discharge the legal duties of the data controller. Elected members will have the use of PTC's email system for both town council and ward data processing, and training is available to ensure that they are able to understand their responsibilities and boundaries. This will enable them to meet their obligations under UK GDPR.

UK GDPR SCOPE

This policy applies to all personal information held in any recorded format such as handwritten notes, email, paper, video or photographic images, in line with the Information Commissioner's Office (ICO) definitions regarding GDPR. It applies to all officers (including non-permanent staff, volunteers and elected members), who process personal data on behalf of PTC. It is a criminal offence to destroy personal information when the purpose of the destruction is to avoid disclosure following a request. It may also be a disciplinary offence to refuse to disclose information entitled to be disclosed under UK legislation.

PRESTATYN TOWN COUNCIL SCOPING EXERCISE

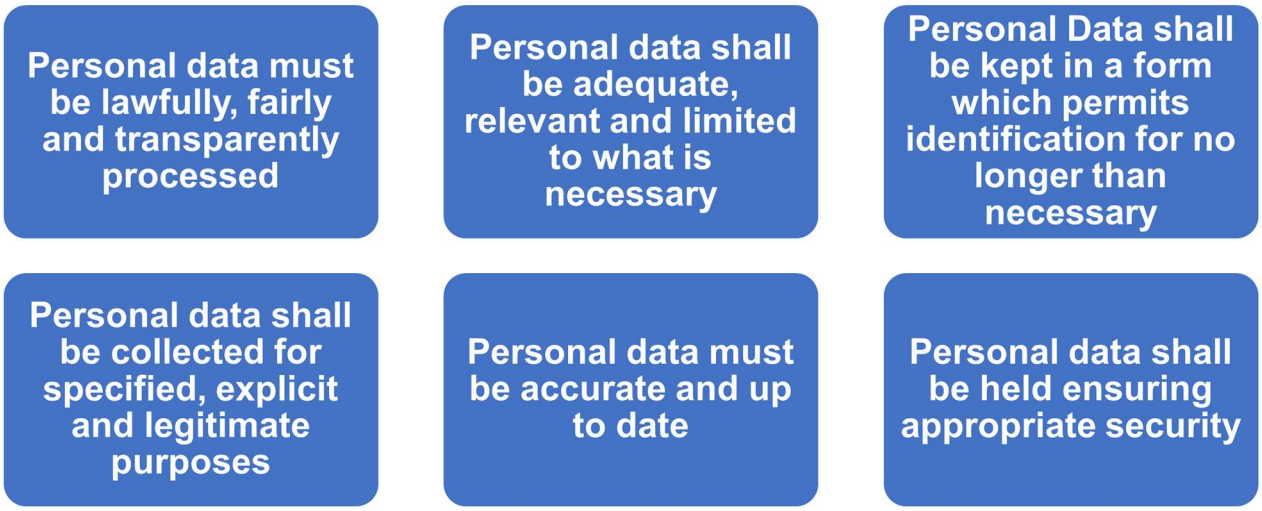
To identify what personal data is held by PTC, what it is used for and who it is disclosed to, PTC undertook a scoping process. The results of the Personal Information Data Audit have been included in **Appendix A**.

PRINCIPLES OF THE DATA PROTECTION ACT 2018

The DPA is underpinned by six fundamental principles, which form a code for the proper processing of personal data.

In the DPA, Processing means anything that is done to or with personal data. This includes but is not limited to collecting, recording, organising, structuring, storing, adapting, altering, erasing or destroying. If we cannot comply with all six principles, Prestatyn town Council should not be processing the data.

The six principles of data protection are:



PTC Commits to:

- Having procedures in place to ensure compliance with all six principles.
- All new staff receiving appropriate data protection training during their induction training.
- All staff undertaking annual refresher training and reviewing guidance as needed.
- All staff being trained to recognise a subject access request and what to do.
- All staff being required to report data security incidents, including 'near misses', to their line manager.
- Where officers deal with data deemed by the Town Clerk (TC) as highly sensitive personal information, providing additional advanced level training where required.
- Responsibility for compliance with this policy on both an individual level and as a collective responsibility for all who manage or handle personal information on behalf of PTC.
- Any breaches of this policy being investigated by the TC and/or their nominated council officer, which may result in disciplinary action being taken and potentially a criminal prosecution in instances deemed to be wilful or deliberate breaches.
- Individuals being informed of the purposes for which their data will be used and the legal ground for processing the information being supplied.
- All appropriate, technical and organisational security measures to safeguard personal information being put in place, including encrypting or ensuring increased security settings of removable devices (such as laptops or mobile phones), and restricting the use of USB sticks in line with PTC's Information Security Policy.

CONSENT

As Data Controller, PTC must be able to demonstrate that consent (by a statement or a clear affirmative action) was freely given, and that this was specific, informed and unambiguous for each purpose that it is being processed.

Prior to giving consent, the individual shall be informed of their right to withdraw their consent at any time. In other words, it should be as easy to withdraw consent as it is to give it (GDPR Articles 4 & 7).

SUBJECT ACCESS REQUESTS

All requests for information should be sent for the attention of PTC for action. People are able to make requests verbally, although PTC would encourage applicants to use the standard application form in order to assist officers in retrieving the correct information and to avoid any confusion. The details can be found in the Subject Access Requests – Procedures & Checklist document (Appendix B).

The standard corporate procedures will apply to all services of PTC. Article 15 of the GDPR provides the right for individuals to be told by the Data Controller the below:

- What data is held about the individual
- What purpose the data is used for
- To be given a copy of the information, subject to other relevant UK legislation
- To be given details of other organisations or people data has been disclose to
- To ask for incorrect data to be corrected (GDPR Article 16)
- To ask PTC not to use personal information about them for direct marketing, unless a Marketing Consent Form has been completed (see **Appendix E**)
- To be compensated, to the extent of UK law, for damage or distress if PTC do not comply with the Act
- To object to decisions made only by automatic means
- To ask the Information Commissioner's Office to investigate and assess if the individual is not happy with an outcome
- To be notified when a personal breach is likely to result in a high risk to a data subject's rights (GDPR Article 34)

PTC will supply this information, providing the request is made verbally or in writing and sufficient information is given by the applicant to enable PTC to locate the information requested.

All such requests must be logged and ensure compliance within legal timeframes and advice on disclosure of subject access requests, with support from legal services as required.

There is no fee applicable for reasonable requests and PTC will respond within one calendar month; this timeframe includes situations where third-party comments are sought. Where comments or consent are not forthcoming, then the law allows PTC to make a decision without such comments or consent. Access to ones' personal information is the cornerstone of the legislation, and this is likely to be of greater weight than third party views, unless there is a genuine legal reason to refuse. Reliance on obtaining third party consent should not be a reason to delay processing the request. The decision on disclosure belongs to PTC.

If the request is complex or multiple, the timeframe may be extended by a further two calendar months. Under such circumstances, PTC shall write to the applicant advising of the circumstances and setting out the reasons as to why.

There is no definition within the Act, but in respect of an 'excessive' request it is generally taken to mean that the effort the organisation would have to expend in complying with the requirement to provide a copy is disproportionate to the benefit to be derived by the individual in receiving it. In such circumstances PTC will consider a refusal of the request and may seek advice from the Information Commissioner's Office.

As the right of access to one's own information is fundamental to data protection law, the circumstances where disproportionate effort can be relied upon will be rare. PTC will provide the information in a permanent format that is understandable to the applicant, unless the supply of such a copy would involve disproportionate effort or the applicant agrees otherwise. Where possible, electronic secure transfer will be encouraged, as this is more secure and more economical to the public purse.

WITHOLDING INFORMATION

There are some situations when organisations are allowed to withhold information, for example if the information is about:

- The prevention, detection or investigation of a crime
- National security or the armed forces
- The assessment or collection of tax
- Judicial or ministerial appointment

An organisation does not have to say why they're withholding information.

COMPLAINTS

If a person believes their data has been misused or PTS has not kept it secure, they should contact PTC and let them know.

If they are unhappy with PTC's response, they can make a complaint to the Information Commissioner's Office (ICO) or get advice from the ICO.

ICO – Monday to Friday 9am to 4:30pm
Telephone: 0303 123 1113
Textphone: 01625 545860

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

FEES

The GDPR only allows PTC to make an administrative charge for requests which are manifestly unfounded or excessive. PTC will, in most cases, refuse such requests and therefore there will be no requirement to raise a fee.

FREQUENTLY ASKED QUESTIONS

More common questions have been identified through the office of the Information Commissioner and general responses have been provided as a guide to requesters. A copy of the Frequently Asked Questions is provided in **Appendix B** and may be provided with a request for a copy of the Subject Access Review – Application Form.

OCCUPATIONAL HEALTH INFORMATION

Employees personal information processed by the Occupational Health Unit will be held under the Data Protection Act 2018 and the Access to Health Records Act 1990.

PRIVACY NOTICES

There is a legal requirement to provide individuals with a privacy notice at the point of collection of personal information. The privacy notice communication needs to be concise and intelligible, using clear and plain language, particularly where the information is addressed to a child.

These should include:

- The identity and contact details of the Data Controller (PTC);
- The purpose of the processing
- The categories of personal data concerned: General (name and contact details); Special: sensitive data, such as racial or ethnic origins, religious or philosophical beliefs, trade union membership, health, sexual orientation, genetic data, biometric data)
- Details of who the information will be disclosed to, more particularly those recipients outside the country or international organisations
- Where possible, the envisaged period of the data being maintained (otherwise PTC must provide the criteria being used to determine the period of retention)
- The right to lodge a complaint with the Information Commissioner's Office
- Clarification of the source of the data if it is not from the data subject

EMAIL USE AND DATA PROTECTION

PTC staff should only use an authorised PTC email account to communicate in respect of Council business and functions. Under no circumstances should staff (including fixed term, temporary, supply, agency or otherwise) use their personal email account to communicate personal information in order to protect all individuals concerned.

In addition, staff shall not send council personal data to their own personal email address without authority and a business reason to do so. Any staff member communicating or transmitting data in breach of this policy may face disciplinary action and place PTC in the position of self-reporting such breaches to the ICO. Highly sensitive information should be communicated via a secure email service such as egress or approved governmental secure email system.

If PTC needs to carry out a type of processing of personal data that poses high risks, there will be a requirement to carry out a Data Protection Privacy Impact Assessment (DPPIA) before the processing takes place. The Information Commissioner's Office can provide guidance on this.

INFORMATION ASSET REGISTER

PTC must keep their section of the corporate 'Information Asset Register' fully up to date. It is a legal requirement under GDPR to maintain such a register, which should be reviewed periodically. PTC is obliged to self-assess its compliance levels and can only do this if it knows what data it holds, where it is, how it is held, how long it is retained, to whom is it disclosed and the lawfulness or powers to process it in the first place.

For any new processing, new systems or additional data collected, PTC should consider whether the Information Asset Register needs to be updated to reflect this change, together with consideration of completing a DPPIA.

CORPORATE RETENTION SCHEDULE

PTC has a Data Retention & Disposal Policy (**Appendix C**) that relates to personal data in all formats. The policy outlines which information should be retained, for how long and under what authority the information is held.

This is followed and regularly revised to meet changes in legislation where they occur.

DATA SECURITY BREACHES

All data security breaches, including both actual and potential incidents, may need to be reported to the Information Commissioner's Office. PTC has a GDPR Reporting and Next Steps Policy (**Appendix D**) that clarifies the procedures when identifying, investigating, recording and reporting such incidents. All reports to the ICO will be made within 72 hours of the breach being identified, where there is a high risk to the rights and freedom of the individual(s) involved or risk of harm to the individual(s) themselves.

OVERSIGHT ARRANGEMENTS AND REVIEW OF POLICY

This policy will be reviewed annually by PTC and the appropriate Committee, to ensure compliance with the legislation at that time. PTC continuously seek to improve procedures within the arena of data security, within the legislation and good practice recommendations.

GLOSSARY

- **"Personal Data"** is any information about a living person which can identify them. This is not only an individual's name and address, but any information which can identify them (directly or indirectly). A phone number or email address is personal data, as too is any other contact information, along with employment or credit history.
- **"Data controller"** is the person or organisation who determines the how and what of data processing.
- **"Data processor"** is the person or firm that processes the data on behalf of the controller.
- **"Data subject"** is the person about whom personal data is processed.
- **"Processing"** personal data means storing or deleting any personal data on a computer, database or in physical files. The word 'processing' covers selecting a name for a mailing list or reading this off a screen during a call, transferring and altering data, etc.
- "**Sensitive personal data or special categories of personal data"** are any of the following types of personal data about a data subject: racial or ethnic origin; political opinions; gender reassignment; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

APPENDIX A

Personal Information Data Audit

BACKGROUND

The Personal Information Data Audit has been prepared to support PTC in meeting the obligations under the General Data Protection Regulations (GDPR).

The purpose of a Data Audit is to clarify what data PTC is obtaining, processing, storing and deleting; including how the data is managed, who has access to it and when it should no longer be held. The Data Audit is an important step in assessing if there are any risks with the way the data is obtained, used and handled.

Description of Data	Obtained From	Where/How Stored Security in Place?	Disclosed to
Councillors Name Home Address Email Address Phone Number(s) Photos	Post election from each Councillor Updated as and when required	On PTC office computer system – password protection to prevent external access, virus protection & security software[1] On office laptop – password protection to prevent all access other than Town Clerk[2] Hard copy in Admin Files held in main office and TC's office at PTC Details included, in part, on PTC website, where agreed with each Councillor	Used to communicate and carry out Town Council functions
Councillors Declarations of interest Register	Disclosure & Registration of Interests Form completed by the Councillor	On PTC office computer system & office laptop – *as above* Hard copy in Admin Files held in main office at PTC Details included, in part, on PTC website	Required to meet Part III of the Code of Conduct for Members and whilst the details may contact sensitive information, it is permitted under the heading of 'substantial public interest'

[1] Huntress Managed Endpoint Detection and Response System
[2] Obsidian have installed virus security protection on the laptop

Description of Data	Obtained From	Where/How Stored Security in Place?	Disclosed to
Employees Name Date of Birth Home Address Private Email Address Phone number(s) Bank Account Details National Insurance No. Salary Details Attendance Records Employment start and finish dates Tax codes Pension details Expense records Medical records DVLA & insurance Employments records Job applications, CVs and references	During recruitment and at time of appointment Employees are asked to provide current details if they change and are formally requested to confirm details annually	On PTC office computer system password protection & virus protection & security software Personnel software – Bright – uses Hard copy in personnel files for all members of the team in office	Used to communicate and carry out Town Council functions Pay details held by on the accounting system, protected by the Acronis Cyber Protect Cloud & through password and security card Pension details held by LGPS Employment records held to meet statutory employment laws
Recruitment Papers for Temporary Roles Name & Adress Contact numbers Pay rates Completed application forms CVs Record of interviews & Decision letters	Collated at time of application and throughout the interview process Request made in decision letter to keep details on file – no confirmation from recipient in file (may be held elsewhere)	Hard copy in file maintained in the main office	

Description of Data	Obtained From	Where/How Stored Security in Place?	Disclosed to
Volunteers Name Address Email address Emergency Contact	Collected at point of contact and maintained for the duration of volunteering duties	On PTC office computer system – password protection to prevent external access, virus protection & security software On office laptop – password protection to prevent all access other than Town Clerk Hard copy in Volunteer File held in main office at PTC	Used to communicate and manage events
Vendors at PTC Events Name Business Address Contact email & phone no.	Collected during negotiations of participation	On PTC office computer system – *as above* On office laptop – *as above*	Used to communicate and manage events
Contractors & Suppliers Name Business Address Contact email Contact phone no.	Collected at point of contact and maintained for the duration of contract	On PTC office computer system – *as above* On office laptop – *as above* Hard copies of quotes maintained in office files to meet documentation regulations	Data used to communicate with supplier during the tender process and if successful
Groups & Organisations Name of Committee members Email addresses of Committee members Contact phone numbers of Committee members	Collected during first contact and updated at subsequent contact Collected at grant application stage	On PTC office computer system – password protection to prevent external access, virus protection & security software On office laptop – password protection to prevent all access other than Town Clerk Hard copies of details where grants applied for maintained in office files to meet Documentation regulations	

Description of Data	Obtained From	Where/How Stored Security in Place?	Disclosed to
Council Minutes Names of Members of the Public Names of debtors	Collected during the meeting Confirmed during preparation for the meeting	On PTC office computer system – *as above* On office laptop – *as above* Hard copies of minutes for maintained in office files to meet documentation regulations Details included on PTC website	Public domain (unless confidential)
Outgoing Correspondence Name Address Email address Contact number	Hard copy taken at point of postage	On PTC office computer system – password protection to prevent external access, virus protection & security software On office laptop – password protection to prevent all access other than Town Clerk Hard copy maintained in HR recruitment files	Held to support manual record of outgoing post – a list kept separately & maintained in office
Incoming Correspondence Name Address	Original copy forwarded to appropriate Department and filed after being processed	On PTC office computer system – *as above* On office laptop – *as above*	

Notes:

- No personal data information is sent overseas – the IT management company, Obsidian, are UK based
- In the event of a potential or actual breach, PTC follows the process in the Reporting & Next Steps GDPR (**Appendix D**) which is line with the Information Commissioner's Office guidance.

APPENDIX B

SUBJECT ACCESS REQUEST – APPLICATION FORM

Full Name: .....

Any other name known by, relating to period of information requested:

.....

Any identifiers, such as account numbers or employee number:

.....

Address: .....

.....

Address during period of time information is being requested (if different from above):

.....

Home Telephone Number: .....

Mobile Telephone number: .....

Email address.....

How would prefer to be contacted?

- ☐ Letter
- ☐ Email
- ☐ Mobile telephone
- ☐ Home telephone

Details of personal data information requested:

From	To	Description of information required

How would you like to receive the information?

- ☐ By email
- ☐ By post

Signed: .....

Name: .....

Date: .....

For office use only:

Date received: Date report due to ICO:

Forward details to Town Clerk Immediately

Appendix B2

FREQUENTLY ASKED QUESTIONS

Can I make a subject access request verbally?

Yes. You can make a subject access request verbally, but we recommend you put it in writing if possible because this gives you a record of your request.

If you are making a verbal request, try to:

- Use straightforward, polite language
- Focus the conversation on your subject access request
- Discuss the reason for your request, if this is appropriate – work with PTC to identify the type of information you need and where it can be found
- Ask PTC to make written notes – especially if you are asking for very specific information
- Check PTC's understanding – ask them to briefly summarise your request and inform them if anything is incorrect or missing before finishing the conversation

However, even if you make your request verbally, we recommend you follow it up in writing (e.g. by letter, email or using the standard form (available on the website under the GDPR Policy or by request from PTC).

Should I use the PTC's standard Subject Access Request form?

Standard forms are not compulsory and are not always provided. However, PTC does recommend using theirs.

Standard forms can make it easier for PTC to deal with your subject access request. The form may:

- Structure your request
- Prompt you to include necessary details and supporting documents
- Let you know the best contact point at the organisation

Can someone else make a request on my behalf?

Yes, you can authorise someone else to make a subject access request for you, however, you should consider whether you want the other person to have access to some or all of your personal information. Depending on the nature of your request, the other person could gain access to information that you may not want to share with them.

Examples of individuals making requests for other people include:

- Someone with parental responsibility, or guardianship, asking for information about a child or young person (for further information, please read our guidance for organisations on requests for information about children)
- A person appointed by a court to manage someone else's affairs
- A solicitor acting on their client's instructions
- A relative or friend that the individual feels comfortable asking for help

PTC would need to be satisfied that the other individual is allowed to represent you.

We may ask for formal supporting evidence to show this, such as written authorisation from you or a more general power of attorney. It is the person's responsibility to provide this when asked to do so.

Should I keep a record of my request?

Yes – whenever possible, we strongly recommend that:

- You keep a copy of any documents or written correspondence for your own records
- You keep any proof of postage or delivery (such as a postal reference number), if available
- If using an online submission form, you take a screenshot before sending

Where relevant documents are not available for you to copy, consider making a written log of your request. This should include key details, such as:

- The date and time of your request
- The location (e.g. if your request was made in person)
- The contact number or submission form you used
- The details of any contacts you have interacted with
- Notes about any personal information you asked for
- Any further information that the organisation may have asked you to provide
- Any reference numbers given to you

This will provide helpful evidence if you wish to follow up your request, raise complaints or complain at a later stage.

APPENDIX C

Data Retention & Disposal Policy

BACKGROUND

While carrying out its various functions and activities, the Town Council collects information from individuals and external organisations and generates a wide range of data/information which is recorded. These records can be retained as hard paper records or in electronic form, however the period of retention must be no longer than is necessary for the purposes for which personal data are processed.

To ensure PTC meets its obligations, the data format, use and retention is considered on a regular basis.

DATA FORMAT

- Contact received from third parties
- Invoices
- Completed application forms
- Planning Applications
- Financial Records
- Declarations of interest
- Registers
- Contract / Deeds
- e-mail communications
- Photographs

DATA USE

- Fulfil statutory or other regulatory requirement
- Evidence events/agreements in case of disputes
- Meet operational needs
- Ensure the preservation of documents of historic or other value

DATA RETENTION

The Data Protection Act 2018, which incorporates the General Data Protection Regulation (GDPR), places legal obligations on organisations who collect and use personal information and gives individuals certain rights of access. In addition, there are stricter requirements in the Act in respect of processing 'special category data'.

The permanent retention of all documents is unlawful and undesirable and a regular 'housekeeping' exercise of reviewing data held and the purpose, particularly where changes have been made to policy or procedures, is necessary to fulfil the obligations within the statute.

There are additional benefits:

- Storage space needs to be maximised in terms of efficiency
- Appropriate disposal of existing documents can free up space
- Reduction of fire risk – in the case of paper records in larger storage areas
- The risk of theft, misappropriation or misuse is not possible if the unnecessary data does not exist

Maintaining a relevant data storage facility reduces risk and improves efficiencies.
The following table clarifies the type of data record held, how long it should be kept and for what reason.

When we dispose of data it must be done with reference to the level of risk should that data become public at any time. The majority of information held within PTC is public, however we use a contract shredding company for all appropriate documents and have an IT Management Company to ensure computer files are disposed of effectively.

TYPE OF RECORD	MINIMUM RETENTION PERIOD	REASON
FINANCIAL RECORDS		
List of payments made	7 years	HMRC
Paid Invoices	7 years	HMRC
Bank Reconciliation	7 years	HMRC
Bank Statements	7 years	HMRC
Bank paying – in books	7 years	HMRC
Cheque book Stubs	7 years	HMRC
VAT records	7 years	HMRC
Budget	7 years	Reference Filed within minutes
Quotations and Tenders	7 years	HMRC
Audited Annual return	Indefinitely	HMRC & Audit
INSURANCE RECORDS		
Certificate of Employers Liability Insurance	40 years from date on which insurance commenced or was renewed	Although no longer a legal requirement the insurers / legal advisers say 40 years is still advisable.
Insurance Documentation including policies	3 years	To cover any claims under Public Liability Insurance as per insurers.
Insurance Claims	6 years	Recorded Information

TYPE OF RECORD	MINIMUM RETENTION PERIOD	REASON
PAYROLL RECORDS		
Payslips / expenses	7 years	HMRC
Tax and NI Records	7 years	HMRC
PERSONNEL ADMINISTRATION		
Employee Letter of appointment	6 years after departure from employment	Consistency
Employee Contract	6 years after departure from employment	Consistency
Personal information relating to Councillors; contact details, bank details, expense claims etc	Maintained for the period they are a Councillor within Prestatyn Town Council, unless maintained under separate authority (for example expenses claims under financial requirements)	Reference
RECRUITMENT		
Recruitment records where candidate did not attend an interview	Securely disposed of at stage identified as no longer required	Reference
Recruitment records for candidates that interviewed unsuccessfully	Securely disposed of at stage identified as no longer required – unless authority provided by candidate to retain for 12 months in the event of a position becoming available	Reference
PLANNING DOCUMENTS		
Planning Applications	After the County Council decision is made	Reference
Planning Decisions	Indefinitely	Included in minutes
LEGAL DOCUMENTS		
Deeds, conveyances and other legal documentation relating to ownership i.e. Title Deeds and leases	Indefinitely	Audit, Management
Contracts not executed as a Deed	6 years	Audit, Management

TYPE OF RECORD	MINIMUM RETENTION PERIOD	REASON
ADMINISTRATION RECORDS		
Approved Minutes	Indefinitely	Archive
Asset Register Current and last competed audit version Audit and management e-mails	Delete routine / trivial emails	Management
Historical Records	Indefinitely	Public Records Act 1958 Archive
Personal data kept for no longer than is necessary for the purpose for which it is held	To be considered in line with particular areas included within this review and with consideration to GDPR guidelines where it is a new scenario	
Register of Members	Whilst a Member	Publication Scheme
Complaints	3 years	Interest

APPENDIX D

GDPR Reporting and Next Steps Policy

REPORTING REQUIREMENTS

If it is believed that a personal data breach has taken place the details must be recorded and a determination made as to whether the report should be submitted to the Information Commissioner's Office (ICO). This policy document complies with GDPR Article 33(5).

Time is critical, as by law **all appropriate reports must be submitted with 72 hours** of the breach being identified, without undue delay. Be aware that not all breaches have to be reported and this document will ensure that appropriate action is taken.

The ICO's main aim is to provide help to organisations to prevent future incidents.

STEP ONE – DON'T PANIC

Not every breach needs to be formally reported, but we do record all potential and low risk cases locally; to improve procedures. The ICO is there to help, support and advise, so that we can understand what has happened and prevent it happening again.

STEP TWO – START THE TIMER

As soon as you are aware a breach may have taken place, advise the Town Clerk (TC) and/or the Data Protection Officer (DPO). This should be carried out both verbally, as a starting point, and by email, to clarify the timing and ensure the appropriate people are aware.

STEP THREE – FIND OUT WHAT'S HAPPENED

The TC and or DPO will pull the facts together and start the Internal Data Breach Report Log. Consideration will be made of the facts; how the incident happened, why the incident happened, how many people were involved, a timeline of events and what actions have been taken so far.

STEP FOUR – TRY TO CONTAIN THE BREACH

The TC and/or DPO will, if possible, take steps recover the data. They will also do whatever they can to protect those who will be most impacted.

STEP FIVE – ASSESS THE RISK

An assessment will be made by the TC/DPO as to what risk of harm there is to those affected: customers, members of staff or service users. This refers to any potential, or actual, harm or detriment it may cause to people.

STEP SIX – IF NECESSARY, ACT TO PROTECT THOSE AFFECTED

Where possible the TC/DPO will give specific and clear advice to people at each stage so they can protect themselves and also clarify what the TC/DPO can do to help them. If the risk is not high, there is no mandatory reason to let people know about the incident.

If the risk is high, then by law, they must be advised without undue delay.

STEP SEVEN – SUBMIT THE REPORT, IF NEEDED

If the breach is reportable access the ICO reporting page report-a-personal-data-breach-form.doc (live.com)

The priority is to let ICO know the details that you have within 72 hours – even if the investigation/resolution is not complete.

INTERNAL DATA BREACH REPORT LOG

Date/time of potential/actual breach	Date: Time:
Date/time potential/actual breach identified	Date: Time:
Deadline for reporting details to ICO if required (within 72 hours of breach being identified)	Date:
Has a personal data breach occurred – has PTC had a security incident that has affected the confidentiality, integrity or availability of personal data?	Y/N
Does the breach involve personal data of living individuals?	Y/N
Who identified the breach?	Name: Employee of PTC? Y/N Councillor? Y/N Member of the Community: Y/N Other (please specify)
How was the breach identified?	Reported by person affected? Y/N Reported by third party? Y/N Other (please specify)
What happened? Provide a description of the facts, using a timeline where appropriate:	
Why did it happen (if known)?	

Can PTC recover the data where possible? If it has been sent to someone in error, can it be recalled, sent back, collected or an email deleted and returned securely? If PTC is not sure where the data is, can steps be retraced? If data has been stolen, for example on a laptop, can it be wiped remotely? Does PTC need to change passwords to prevent further access?	Y/N What steps are being taken to recover the data? Was the retrieval successful? Y/N
Is there a high risk to rights and freedom of the individual; potential or actual? To identify the risk level, is there chance of harm, or potential harm or detriment to people; safeguarding issues, identify theft or significant distress?	Y/N
Is there a risk to individuals; potential and/or actual?	Y/N
Can we protect those affected? Have the individuals been advised of the incident? If not, please clarify why not. PTC is able to let the people affected know, advise them to use strong passwords, look out for phishing emails or fraudulent activity on their accounts. There needs to be a balance between telling people about the incident and not causing unnecessary worry. If there is a high risk of harm, PTC must advise the individual, by law, without delay.	Y/N Y/N
Steps for prevention of reoccurrence - What could/should PTC have done differently? - Does PTC need to update any processes or procedures to prevent a repeat incident? - If so, which details need to be amended? - Confirm date revisions made	Date:
Is a report required to the Information Commissioner's Office?	Y/N Y/N

- Is there high risk to individuals' right or freedom or to the individual/s themselves? - Do we believe the ICO may receive a complaint about the incident (if so, the report will prepare ICO)? Date/time report made: Attach screen print from ICO to confirm report made.	Date: Time: Y/N
Reassess where necessary, particularly if new information comes to light, and provide additional details to the ICO where appropriate The ICO can be contacted on 0303 123 1113 (Mon-Fri 9am – 5pm)	

APPENDIX E

GDPR Marketing Consent Form

PRESTATYN TOWN COUNCIL

GENERAL DATA PROTECTION REGULATION (GDPR) CONSENT FORM

The GDPR guidelines clarifies that PTC must disclose to individuals when we are collecting and using personal date. Such information consists of name, address, telephone number(s) and email address if you have provided them. This information will usually be solely for purpose of Town Council communicating with you.

You may ask that PTC deletes any incorrect information or information that it no longer requires.

Within the terms specified by the GDPR legislation, we need you to complete the form below to give your consent to us to collect, use and store your personal data and to use it as part of our events and marketing campaigns that may benefit you and your business or interests.

Please consider the statements below and (✓) your chosen option:

1. I can confirm that I understand how you use and store data, and I give my permission to PTC to collect, use and store my personal data for purposes in accordance with the GDPR guidelines.

☐ **YES** ☐ **NO**

2. I agree that you can contact me for marketing purposes, via post, email, telephone and/or text.

☐ **YES** ☐ **NO**

3. I agree that you can store and use photographs or video taken of my business on your website and social media platforms, such as website, Instagram, Facebook and Twitter, that is constructive and positive, to support my business.

☐ **YES** ☐ **NO**

4. I would like to sign up to the Local Directory.

☐ **YES** ☐ **NO**

5. I agree that PTC can use my business pictures on social media and the website and the Local Directory.

☐ **YES** ☐ **NO**

If you are happy for PTC to promote your business, what would you like them to include?

Owner's Name: _____

Business name: _____

Business Address: _____

Business Category: _____

Contact Number: _____

Email Address: _____

Social Media Addresses:

Facebook-	***Twitter-***
Website-	***Instagram-***

Signed:..... Date: .....

Please return this form by email to events@prestatyntc.co.uk or return to

PTC Offices, 7 Nant Hall Road, Prestatyn LL19 9LR

01745 857185