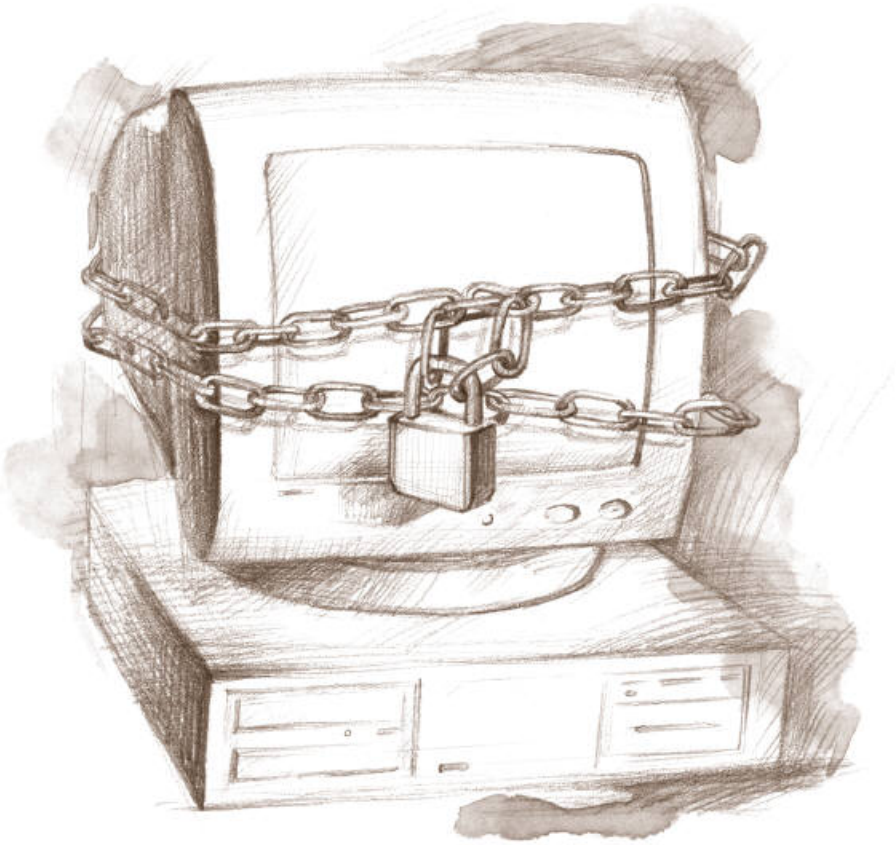
Rhyl Town Council

Data Protection
Policy and Procedures



August 2006

Data Protection Policy

Policy Aim	3
Summary of Key Policy Decisions	3
Policy Statement	4
Scope of Policy	4
Procedures and Guidance	5
Disclosures of Information	5
Subject Access Requests	5-6
Exemptions	6-7
Consent	7
Information Subject to Specific Rules	8
Enforcement and Sanctions	8
The Internet and Email	9
The Corporate Disclaimer	9
Where can I seek further advice?	10
Definition of Terms Used in this Policy	11-12
The 8 Principles of the Act	13-15
Notification	16
Councillors	16
Responsibilities	16

Policy Aim

The purpose of this policy is to ensure that all employees and members comply with the provisions of the Data Protection Act 1998.

Summary of Key Policy Objectives

- To provide employees and members of Rhyl Town Council with a basic handbook/guidance document on the main principles of Data Protection legislation.
- To offer guidance upon how Rhyl Town Council employees can obtain assistance with more complex data protection issues which are not covered within this policy.
- To establish a clear process for receiving requests for data from individuals pursuant to Section 7 of the Data Protection Act 1998, and to advise employees on the processes to be followed when dealing with such requests.
- To establish a consistent charging regime for subject access requests.
- To increase awareness and understanding of the main provisions of Data Protection legislation and ensure compliance with its provisions.

Policy Statement

Introduction

The Data Protection Act 1998 ('the Act') became part of UK law on the 1st March 2000. The Act's purpose is to protect the rights of individuals (including members and employees - past and present) and to enable them to have access to information that might be held about them by companies, local authorities and other organisations. The Act also places an onus upon organisations which hold information about individuals to safeguard that information and to deal with information about individuals in a certain way. The Act restricts the way in which information about others can be used and shared within and outside the organisation. In addition, all of the various types of personal information that is processed by an organisation has to be formally notified to the Information Commissioner.

The general rule is that any organisation or individual which processes personal data must comply with the provisions of the Act.

Although the Act has now been in force in the UK for a period of some years, there remains relatively little case law about the Act and how its provisions should be interpreted, and there continues to be, to some degree, uncertainty and confusion about how the Act affects those who use information about individuals in the course of their daily work.

It has to be said that there is an increasing wealth of information about the Act – particularly on the Internet – and in the guise of Guidance notes produced by the Information Commissioner. This information, whilst useful, is to a large degree indicative of the opinions of various individuals, and does not of itself provide definitive answers for staff relative to their areas of work. This policy document should provide a consistent handbook for employees of Rhyl Town Council who deal with information about people within their sphere of work. It is essential that all members of staff are fully aware of data protection issues given that they could be prosecuted for failing to adhere to the provisions of the Act and such failures could also form the basis of action against them in accordance with the Town Council's own disciplinary procedures.

Scope of Policy

The provisions of this policy apply to and should be observed by all Rhyl Town Council employees and members. The policy also has an impact upon members of the public in the methods in which the Town Council deals with the personal information of its constituents and other persons with whom it is in contact. This policy is not intended to be an authoritative and complete guide to all of the issues that arise pursuant to the Act, but hopefully will contain the answers to some of the simpler questions and at least offer guidance about how employees can seek further assistance to help them answer queries as and when they arise.

Procedures and Guidance

Disclosures of Information

Quite often, you will be approached by external organisations and individuals for information which you may hold about specific individuals; e.g. Inland Revenue, Denbighshire County Council and voluntary organisations. You must always bear in mind that the person making the enquiry may have no right to the information being sought, and you will therefore need to carefully consider whether or not you should disclose the information being sought. You will, in each case, have to consider the following points:

- Rhyl Town Council holds a lot of personal data and any disclosure of personal data must comply with the law.
- Proof of the identity of the individual making the request should be requested. If you disclose the data illegally, you could be at risk of committing a criminal offence and could be prosecuted.
- Has the individual who is the subject of the data consented to the disclosure of the information in these circumstances?
- Does the information make reference to third parties who can be identified from that information? If so have the third parties consented to the release of the information?
- Does the information fall within any of the categories of exempt information referred to in this Policy?
- Do you have authority to disclose personal information? If not, seek advice from the Town Clerk.

There are instances however where you might have to disclose the personal information. Some of those instances are:-

- Pursuant to the provisions of a Court Order
- Various statutory bodies and the Police can obtain warrants to require disclosure.
- There is sometimes a legal duty to disclose (eg. public registers). In these cases, you should always ensure that you request full details of the legal basis for the request and consult with the Town Clerk if necessary. You should keep a copy of what is disclosed and to whom.

Subject Access Requests

Section 7 of the Act gives individuals the right to make a request to Rhyl Town Council for access to any personal data that the Council may hold about them. This is often referred to as a Subject Access Request. The Town Clerk is responsible for dealing with Subject Access Requests and all such requests should immediately be forwarded to the Town Clerk upon receipt.

Subject Access Requests must be made in writing and must clearly specify the information that is requested. The Council is allowed to ask for further clarification and assistance in order to locate the information and to comply with the request. A maximum fee of £10.00 may be levied upon the person making the request. It is imperative that subject access requests are forwarded to the Town Clerk immediately upon receipt as the Town Council

only has 40 days within which to respond to such requests. The Town Clerk should acknowledge receipt of the request as soon as possible.
When answering a Subject Access Request, the individual in question must be informed of the following:-

- Whether personal information about them is processed.
- Details about what personal information is processed, and for what purpose.
- Who the personal information may be disclosed to and where it was obtained from (if known).
- A copy of their personal information.
- An explanation of the decision processes involved if significant decisions are made solely by automatic means.

If there are references to any third parties within such personal information the Town Clerk must write to those third parties to seek their consent to the release of the information. If consent is not forthcoming, consideration needs to be given to determine whether or not the information should be released - this involves counterbalancing the rights of the individual to have access to data about them against the right of the third party to their own privacy. Legal advice should be sought when considering such matters. Further guidance on dealing with Subject Access Requests may be viewed on the Information Commissioner's website.

Exemptions

The Act states that in certain circumstances, personal data may not be disclosed. In addition, the Act says that, in certain situations, personal information should be disclosed to third parties/organisations. In some circumstances, disclosure would be a breach of the Act; however if a particular disclosure falls within an exemption in the Act, then you will not be in breach.
The exemptions found within the Act are fairly complex and somewhat restrictive. Exemptions must never be used as a means of avoiding disclosure and should only be relied upon in circumstances where the use of an exemption can be justified, if the Council were challenged. You must approach the application of any of the Act's exemptions on a case by case basis - they must never be used in a blanket-type approach.
The various exemptions found within the Act are listed below; however you must seek approval from the Town Clerk and/or legal department before seeking to rely on any exemption.
Section 28 - National Security
Section 29 - Crime & Taxation
Section 30 - Health, Education & Social Work
Section 31 - Regulatory Activity
Section 32 - Journalism, Literature & Art
Section 33 - Research, History & Statistics
Section 34 - Information available to the public by or under an enactment
Section 35 - Disclosures required by law or made in connection with legal proceedings
Section 36 - Domestic Purposes

Schedule 7 – Confidential References given by the Data Controller;
Armed Forces, Judicial Appointments and Honours, Crown employment or Ministerial appointment, Management Forecasts, Corporate Finance Negotiations, Examination Marks, Examination Scripts, Legal Professional Privilege.

Consent

In many cases, it will be possible to process an individual's personal data because that individual has consented to the processing. If you are ever uncertain whether or not you should process information about any individual, you should abstain from doing so, or alternatively seek their consent to the processing. In the majority of cases, and particularly when using standard forms to gather data, you will find a signed statement of consent to their information being used and processed in a particular way. This can often be a useful method of ensuring that you have the individual's consent to what you propose to do with the information.

The Act does not prescribe that written consent has to be sought, but does require any consent to processing to be given in a fully informed manner and for consent to be provided freely, and without duress. This effectively means that the person giving the consent must fully understand what they are consenting to and this requires you to fully explain to them why you want the information, what you intend to do with it and who else is likely to have access to it. The individual must not be forced in any way to giving their consent – such consent could be deemed ineffective in law and could be a breach of the Act. If an individual does not wish you to carry out any processing, and they make you aware of this, you should not carry out the processing and seek assistance from the Town Clerk.

In certain cases, you will be dealing with a person over the telephone, and you will therefore be seeking to obtain an individual's oral consent to the processing. Whilst the Act does not specifically prohibit you from relying upon oral consent, it is always preferable to obtain a person's consent in writing. If you have to rely upon oral consent, you must ensure that you fully record the contents of the conversation that took place, making a note of the time and date of the conversation and who took part in the discussion. You should also confirm that you fully explained what you were intending to do with the information, and that you were satisfied that the person giving the consent fully understood what you were intending to do with that information. You are also advised to follow up the conversation in writing as soon as possible.

Information Subject to Specific Rules

The Act makes specific reference to various types of personal information as being of such a nature that it needs to be treated in a particular manner. In addition, both the Welsh Assembly and the Information Commissioner have issued specific guidance on particular issues and types of information so you need to check whether any special rules or good practice methods apply to a specific type of personal data which you are intending to process before any processing is carried out.

Enforcement and Sanctions

The person who is responsible for ensuring that the provisions of the Act are properly complied with is the Information Commissioner. The Information Commissioner (previously the Data Protection Registrar and Data Protection Controller) is appointed by the Government to act as the Act's independent regulator.

The Information Commissioner has wide powers to investigate complaints by individuals that the Act's provisions have been breached. The Commissioner may also issue Enforcement Notices which effectively warn the recipient that they may be in breach of the Act and prescribes them to take certain steps to remedy the situation. The Commissioner also has the power to search premises and documents to ascertain whether any breach of the Act has occurred, and may also institute criminal proceedings against either an individual or a corporate body.

The Act creates a number of criminal offences. These include obtaining, disclosing or procuring the disclosure of personal data without the data subject's consent, selling personal data obtained in contravention of the Act. Sanctions include a fine of up to £5,000.00 and costs in the Magistrates Court or an unlimited fine in the Crown Court.

It is therefore essential that all members of staff are fully aware of data protection issues. Individual members of staff could be prosecuted for criminal offences such as failing to adhere to the provisions of the Act and such failures could also form the basis of disciplinary procedures against the individual member of staff in accordance with the Town Council's own disciplinary procedures.

It is imperative that all Town Council employees are responsible for making sure that personal information is properly handled. The Town Clerk is responsible for ensuring that all employees are properly trained in data protection issues and are aware of the existence of this policy and have access to a copy, and should carry out intermittent quality control checks for checking upon compliance with this policy. If any member of staff is unsure whether or not they are acting within the scope of the provisions of the Act, they should seek advice and guidance in accordance with the section "Where Can I Seek Further Advice?" of this Policy or by consulting with the Town Clerk.

The Internet and Email

As we have already discovered, the Act controls the use of personal data. We have also established that if an e-mail contains personal information about an individual, then the e-mail is potentially covered by the provisions of the Act. When using the e-mail facility therefore, you need to bear in mind the 8 Principles of the Act. In particular, you need to ensure that the information contained in e-mails is used in a fair and lawful manner, that you do not process personal information via e-mail unless this is consistent with the purpose for the which the information was collected, that the information is accurate and kept up to date as far as possible, that you destroy information that is no longer accurate or not required, and that you generally do not send information outside the area of the European Economic Area. In reality, great care should be taken even when sending material outside the United Kingdom, and this practice is generally discouraged.

The Internet is a large network of unregulated computers. It is not generally secure and the accuracy of information found on the Internet cannot be guaranteed. It is important to remember that anyone in the world who has access to the Internet can view information placed on a website. Clearly, if personal information (including photographs) is placed on the Internet or Intranet, the subject of the information/photograph will, in the vast majority of cases, need to have given their written consent to the information being put on that site. If you are unsure as regards what information can be legitimately put on the website you should contact the Town Clerk. In general, care should be exercised when putting material on the Internet. Only authorised officers are able to put material onto the Council website, and before any additions any data protection implications need to be given careful consideration. Seek advice from the Town Clerk if necessary.

The Corporate Disclaimer

The Town Council includes a Corporate Disclaimer on specific forms when collecting personal data to alert the reader to the provisions of the Act.
The Disclaimer should appear on all documentation which is issued to the public for the purposes of collecting information about them or in order to enable the Council to provide a service to them. Officers are however advised to consider whether the Corporate Disclaimer works for the purposes of their document in all cases. Otherwise they should seek advice from the Town Clerk.
A copy of the Corporate Disclaimer is reproduced below:-

Data Protection Act 1998 - I understand that the information supplied by me on this form may be disclosed by Rhyl Town Council to other persons or bodies with an interest in, or involved with, the business, retail, charitable or voluntary sector.

Where can I seek further advice?

Rhyl Town Council is committed to complying with its statutory duty to observe the provisions of the Act. The Council's employees must possess a basic understanding of the provisions of the Act, and this document seeks to provide such an understanding.
However, the Act is complex and applying its provisions to real life situations can be very difficult. The Council recognises that it must take it legislative duties seriously, and has appointed the Town Clerk as the Data Protection Officer. He has overall responsibility for ensuring that the Town Council conforms with its statutory requirements and does not breach the provisions of the Act.

The Town Clerk has a day-to-day responsibility to answer general queries on the Act and also deals with Subject Access Requests under section 7 of the Act. Employees are able to discuss any Data Protection concerns they may have with the Town Clerk.

In addition, the Information Commissioner has established a telephone enquiry line which can be used to seek advice and assistance on issues and to gain an understanding of the Information Commissioner's viewpoint on certain issues. Employees should note however that the advice given should be double-checked with the Town Clerk. The Enquiry Line is not a free legal service and the advice provided should be used only as a guide. Employees should seek advice from the Town Clerk if they require specific legal advice on any matter and before they release any personal data.

Please note however that personal information should be withheld if:

- the person asking for the information does not have lawful authority to do so
- the data subject did not and still does not expect the personal information to be disclosed
- the data subject does not want the records to be disclosed

Sometimes, personal information is requested for use in pending criminal proceedings. In all such cases, seek the advice of the Town Clerk before you disclose anything.

Employment Records

Employment files will contain potentially sensitive personal information about the Town Council's members of staff. Access to those files should clearly be strictly on a need to know basis and access should be made solely for employment and personnel purposes.
The Information Commissioner has published Guidance on issues affecting personnel and employment records. The Guidance is known as The Employment Practices Code and can be downloaded from – www.informationcommissioner.gov.uk.

Definition of Terms Used in this Policy

The Data Protection Act 1998 ("the Act") is a complex piece of legislation, and in order to gain a basic understanding of its provisions, consideration must first be given to the meaning of the most important definitions that the Act uses.

Understanding the meaning and scope of the definitions should help you interpret the Act's provisions correctly and in a consistent manner.

Below is a list of the main definitions found within the Act. The text in italics has been directly quoted from the Act itself. If you need further assistance in understanding the impact of these definitions when applying them to a specific problem, you should contact the Town Clerk. Please note that requests by individuals for information about themselves and how such requests should be dealt with is discussed further in "Subject Access Requests" of this policy.

Data

information which -

- is being processed by means of equipment operation automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- or does not fall within the above definitions but forms part of an accessible record"

Personal Data

This is a key definition – "data which relate to a living individual who can be identified either from those data; or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller; and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive Personal Data

Means personal data consisting of information as to;

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

Please note that the Secretary of State has the power to extend this list at any time, and that additional requirements and obligations are placed upon the Council when dealing with such information.

Data Subject
Means an individual who is the subject of personal data

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

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available;
- alignment, combination, blocking, erasure or destruction of the information or data

Data Controller
“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 to be, processed”

Data Processor
“Any person who (other than an employee of the data controller) who processes the data on behalf of the data controller”

Relevant filing System
“Means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible”

These definitions are used throughout this policy.

The 8 Principles of the Act

If you are processing an individual's personal data, and if that data is manual (paper or hard copy), automated (computerised, including e-mail and faxes) or accessible records (eg. Accounts, town guide, civic guest lists, or a public record to which the public is entitled to access by virtue of other legislation) the Data Protection Act 1998 will apply.

Once you have determined that the 1998 Act applies to what you are doing, you must comply with the 8 Principles of the Act. The 8 Principles are intended to ensure that information about individuals is dealt with properly. If you follow the Principles of the Act you should be able to avoid breaching any of its provisions.

The Act's 8 Principles are reproduced below, along with additional commentary and tips in italics to help you comply with each principle:-

1st Principle

Personal Data shall be processed fairly and lawfully.

It is good practice to process information with the individual's consent, so seek their consent to the processing, wherever possible and preferably in writing. Even where individuals give their information voluntarily, ask them to agree that you can use it. Record this action in writing.

We all expect personal information to be handled properly by organisations. Complying with the provisions of this principle will involve telling the person whose information is being processed that you have the information at an early stage - preferably before you start processing the information. You should also tell the data subject how and why the information is to be used (eg. to include their information in the Town Guide). You should confirm who will be processing their personal information and also give them any other information that they need to understand how their information will be used. It is good practice to tell them who they should contact if they have questions about the information that is to be processed. If you are under a legal obligation to process their information, you should clearly explain that this is the case.

Local Authorities are creatures of statute. Essentially, we can no nothing unless parliament has given us a right to do so. You will therefore need to be familiar with the law under which you are working and what gives the Town Council the right to carry out any particular activity. In essence, do not do anything which the Council has no legal power to do. If you are in doubt, seek advice from the Town Clerk.

2nd Principle

Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

To help you comply with this principle, you should tell the person whose information is to be used exactly what it will be used for. You should process personal information only for the purposes for which that information was

originally obtained. You should avoid using that information for purposes which are significantly different from those it was collected for and you should not disclose such information for other purposes unless an exemption applies.

3rd Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
This principle requires you to consider carefully what information you need to carry out the function that the information is required. You should not ask for information excessive to what is actually needed. (eg. you would not need someone's age for the purposes of processing a complaint that their bins had not been emptied). Do not collect personal information just because you have done so in the past and because it may be useful to have in the future and try to review what information you hold, and why, at appropriate intervals. Please note that information must be disposed of and/or destroyed in line with the disposal and archive retention period determined by the Town Clerk.

4th Principle

Personal data shall be accurate, and where necessary, kept up to date.
This principle requires systems to be put in place so that information is periodically checked to ensure that it is up-to-date. You should also correct any inaccuracies found and update records if you are alerted to their inaccuracy.

5th Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Documents should only be retained for as long as they are necessary. This will be reviewed periodically by the Town Clerk. It should also be borne in mind that information should be destroyed in a responsible manner - eg. shredding sensitive information etc.

6th Principle

Personal data shall be processed in accordance with the rights of data subjects under the Act.
Please see "Subject Access Requests" of this Policy for further explanation of the right of individuals to have access to their personal information. In addition, individuals have the rights to prevent processing that is likely to cause them damage or distress, the right to prevent processing for the purposes of direct marketing and to seek a Court Order to order the Council to rectify, block, erase or destroy personal information which is inaccurate. There is also a right to compensation if the Council fails to comply with any of its obligations under the 1998 Act and cause damage or distress to the individual.

Also individuals have the right to require the data controller not to make decisions which significantly affects the individual solely by automated means. You should seek further advice on the rights of individuals from the Town Clerk should queries arise as the extent of these rights will vary from situation to situation.

7th Principle

Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

The purpose of this Principle is to ensure that the organisation has adequate measures in place to safeguard the security of personal information, and to use and dispose of such information in a responsible manner. Such measures should prevent unauthorised or unlawful processing by inappropriate personnel and should safeguard the data from accidental loss and/or damage. Employees have a responsibility to look after the data which they process and not to process data that they are not authorised to work with. Computer systems should have adequate security measures in place and disclosures of personal information should be strictly controlled and documented by the person making the disclosure. Details to be documented would include that of the date, the name and address of the person making the request and proof of their identity, the name and position of the officer disclosing the information and a copy of the information disclosed. Further advice can be sought from the Town Clerk.

8th Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures that an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
The Act precludes data from being passed outside the EEA unless there are adequate security measures in place. In practice, it is not advisable to send information outside the United Kingdom (eg. via the Internet, e-mail or post) without the consent of the individuals involved. There are circumstances where this could be done without consent - seek further advice on this.

Notification

The Act requires all data controllers to notify the Information Commissioner as regards the information which they process. The data controller must supply certain information to the Information Commissioner who maintains a public register of what each Data Controller processes. The entry for each organisation will show what information they hold and what they process, where it gets the information from and what it does with that information. Data controllers are under a duty to keep the register accurate and up to date.

The entry in respect of Rhyl Town Council is updated periodically and the Town Clerk is responsible for keeping the entry up to date and dealing with all notification enquiries and requirements. The entry for Rhyl Town Council can be viewed on the Information Commissioner's website – www.informationcommissioner.gov.uk. If members of the public ask what information has been notified in respect of the Council, they should be told about the existence of the register, and that it can be viewed on the Information Commissioner's website. They should also be told that they may order a copy of the entry from the Information Commissioner by contacting them directly. If any member of staff in the Council sets up a new system which involves processing personal data (be that system manual or electronic), they should immediately inform the Town Clerk so that consideration can be given to whether the current notification affecting the Council needs to be extended to cover that additional activity.

Councillors

The question of whether individual Councillors have to notify the Information Commissioner has been a subject of some discussion in the past. The Information Commissioner has issued an Advice Note for Councillors upon their use of personal data and notification which can be viewed on www.informationcommissioner.gov.uk

Councillors could be regarded as data controllers if they process personal data electronically or manually. They need to initially determine in what capacity that they process personal data. When Councillors act on their own behalf, they are likely to have to notify in their own right - eg. the processing of personal data in order to timetable surgery appointments or progress complaints made by local residents. A Guidance Note on disclosing personal data to elected representatives can be found on www.informationcommissioner.gov.uk

Responsibilities

Rhyl Town Council is committed to complying with its statutory duty to observe the provisions of the Act. The Authority's officers and members are ultimately responsible for complying with the Act.

This policy will be regularly reviewed to ensure that it remains up to date, effective and takes account of emerging good practice. Where new legal directions come into force, the policy will be renewed in line with the commencement date of that legislation.