POLICY TITLE

Information Security incorporating - Data Protection, Freedom of Information and Records Management.

REVISION DATE

October 2020

REPLACES POLICY

4th April 2018

POLICY AIM

To set guidance in respect of the use, storage, access, security, retention and disposal of council data, information and records.

EXECUTIVE SUMMARY

This policy has been updated due to the new legal framework in the General Data Protection Regulations (GDPR), applicable from May 2018.The Policy is informed by and works within the following legislative and regulatory framework:

General Data Protection Regulations – regulations intended to strengthen and unify data protection for all individuals within the European Union.

Regulation of Investigatory Powers Act 2000 are corporate procedures relating to the authorisation of Covert Surveillance activities and requests for data from communications providers, in accordance with RIPA (Regulations of Investigatory Powers Act) legislation.

Environmental Information Regulations enables an applicant to access environmental information. They are restricted to information held by/on behalf of public authorities and those bodies carrying out a public function.

Freedom of Information Act enables an applicant access to information which is held by/on behalf of public authorities and those bodies carrying out a public function, and, which **does not** fall under either of the access regimes listed above i.e. personal information or environmental information.

Re-use of Public Sector Information Regulations provides public authorities with the option to charge/impose conditions, to an applicant, on the re-use of its Freedom of Information Act 2000/Environmental Information Regulations 2004 information for commercial purposes.

Records Management is about making sure that public authorities manages its information so that employees can readily locate the correct information they need, at the time they need it.
The **Privacy and Electronic Communications Regulations** May 2011

POLICY STATEMENT

General Data Protection Regulations (GDPR)

The Council is required to gather and process information about its staff and people in the community in order to operate effectively. This will be done in accordance with the General Data Protection Regulations and other related government legislation.

The Council, acting as custodians of personal data, recognises its legal duty to ensure that all such data is handled properly and confidentially at all times, irrespective of whether it is held on paper or electronic means.

GDPR controls how your personal information is used by organisations, businesses or the government. Detailed information on how your personal data is used by the Skegness Town Council can be found on the relevant privacy notice, these are issued when collecting data, published on the Councils website and available from the Town Council office.

Everyone responsible for using data has to follow strict rules called 'principles'. Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner
- collected for specifies, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposed for which the personal data are processed
- processed in a manner that ensures appropriate security of the personal data

Article 5(2) requires that the controllers shall be responsible for and be able to demonstrate compliance with these principles.

GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

The GDPR gives you the right to find out what information the government and other organisations stores about you. You may ask the organisation to remove or correct information stored about you.

The organisation is legally required to give you a copy of the information they hold about you if you request it. You have the right to complain to the Information Commissioner's office if you think there is a problem in the way an organisation is dealing with your data.

For all enquires and requests in relation to the processing or control of your data please contact:

The Town Clerk
Skegness Town Council
Tower Gardens Pavilion
Rutland Road
Skegness
PE25 2AX

The Town Council must also appoint a Data Processing Officer (DPO) to assist the Town Council to monitor internal compliance with the GDPR. Please contact:

Data Processing Officer
Skegness Town Council
Tower Gardens Pavilion
Rutland Road
Skegness
PE25 2AX

When information can be withheld

There are some situations when organisations are allowed to withhold information, eg if the information's about:

- the prevention, detection or investigation of a crime
- national security or the armed forces
- the assessment or collection of tax
- judicial or ministerial appointments

An organisation doesn't have to say why they're withholding information.

Actions

By following and maintaining strict safeguards and controls, the Council will:

- acknowledge the rights of individuals to whom data relates and ensure that these rights may be exercised in accordance with the Regulations;
- ensure that both the collection and use of personal data is done fairly and lawfully;
- ensure that personal data will only be obtained and processed for the purposes specified;
- collect and process personal data on a need-to-know basis, ensuring that such data is fit for the purpose, is not excessive, and is disposed of at a time appropriate to its purpose;
- ensure that adequate steps are taken to ensure the accuracy of the data;
- ensure that for all personal data, security measures are taken both technically and organisationally, to protect against damage, loss or abuse;
- ensure that the movement of personal data is done in a lawful way, both inside and outside the Council and that suitable safeguards exist at all times.

The Council will be able to demonstrate compliance in regard to the above actions.

Enablers

In order to support these actions the Council will:

- ensure that all activities that relate to the processing of personal data have appropriate safeguards and controls in place to ensure information security and compliance with the Regulations;
- ensure that all contracts and service level agreements between the Council and external third parties, where personal data is processed, make reference to the Regulations as appropriate;
- ensure that all staff acting on the Councils behalf understand their responsibilities regarding information security under the Regulations, and that they receive appropriate supervision so that they carry these duties out effectively and consistently and are

- given access to personal information that is appropriate to the duties they undertake;
- ensure that all third parties acting on the Council's behalf are given access to personal information that is appropriate to the duties they undertake and no more and with the consent of the data subject if needed to lawfully process the data;
- ensure that any requests for access to personal data are handled courteously, promptly and appropriately, ensuring that either the data subject or his/her authorised representative has a legitimate right to access under the Regulations, that the request is valid, and that information provided is clear and unambiguous;

review this policy and the safeguards and controls that relate to it regularly, to ensure that they are still relevant, efficient and effective.

Who do we share information with?

Depending on the original purpose for which it was obtained and the use to which it is to be put, information may be shared with a variety of services other organisations that provide services on our behalf.

In all of these examples the information provided is only the minimum necessary, to enable them to provide services to you.

Personal information about you may also be provided to Government departments, where we are required to do so by law, or to other local councils.

Information about you may also be provided for statistical research. This will not include your name and address unless you have given us permission to provide the information.

What sort of information do we hold?

The personal information held will depend on the service being provided. Basic information plus a note of the service provided, decisions regarding the provision, and any correspondence and meetings between you and the Council may appear in records. Data relating to specific services including property details and extent of proposed alterations with regard to planning.

How do we keep the information, and who is responsible?

The information is kept on secure computer systems and in secure manual filing systems. Maintaining the record and keeping it secure is the responsibility of Skegness Town Council.

Are the records confidential?

The Council's employees have a duty of care when providing services. This includes respecting the right to confidentiality and ensuring that information about you is only used and given to others for the purposes of the service being provided. Care is taken to ensure

that third parties cannot access the information without permission and that data about you is not disclosed - to third parties or others - without your consent, except as outlined above in ‘Who do we share information with’.

How long are records about you held?

Normally, your records will be kept only for as long as the service is provided to you, or as is required by law (e.g. financial transaction information is kept for 7 years).

How do you ask to see your information?

You can write to the Council, addressing the letter to the Town Clerk and stating that wish to make a subject access request. When you do so you must provide your name and address; proof of identity; details of the services you are receiving; and any other information, such as date of birth, you think may help the Council find your information.

What information will you receive?

All of the personal information we hold about you on both our computer, and manual record systems. You will also be given a description of the purposes for which we process your data, a list of those to whom we disclose the data, and information about sources where this is available.

Can you see information about members of your family or any other person?

You may not see information about other persons, unless they have given their consent.

Will you be charged a fee for information provided?

No, no charge will be made for providing this information.

How long does it take to provide you with the information?

The Council must respond within 30 days of receiving your request. The 30 days starts from the date on which your written request is received by the Council.

What should you do when you get the information?

You should check it to ensure that you have received all of the information to which you are entitled, and to make sure it is correct.

What do you do if the information provided is incorrect?

You should tell the Council that the data is incorrect and ask them to correct it. Whenever we are in contact with you we will check the accuracy of your data. If you have an allotment or grave it is important you inform us of your up to date contact details.

If the Council does not correct the information you may also appeal to the Information Commissioner or the courts. These organisations have the power to order the Council to correct data.

What can you complain to the Commissioner about?

You can complain to the Commissioner if you consider the Council has breached any of the requirements of the General Data Protection Regulations. **Information Security**

Physical Security

Adequate and practical access controls will be provided in all areas in which personal and business data is stored or used. Unattended rooms will be secured at all times with window blinds and locked doors as a minimum security requirement.

All documents disclosing identifiable information will be transported in sealed containers e.g. envelopes.

Within their level of authority, staff will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as, laptop computers, will not be left unattended or unsecured and paper records will not be left within public view.

The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment e.g. adequate ventilation for computers servers, appropriate fire precautions where paper records are stored, controlled access doors.

Logical Security

All computerised information and systems must be regularly backed up to a secure environment. Appropriate staff only will be allowed access to appropriate levels of data within the systems. Councillors will not be granted access to personal data other than under controlled disclosures for decision making purposes during meetings.

All computerised information systems containing confidential information will be password controlled.

All passwords will be treated with the strictest confidence and users will not divulge their password to any unauthorised person. All sensitive data will be password protected.

Data Protection Impact Assessments

Data protection impact assessments (also known as Privacy Impact Assessments) will take place when data processing poses a high risk to the rights and freedoms of individuals or when a new technology is used to process and collect data.

What happens in the event of a data breech?

Any data breech will be reported to the Town Clerk and Data Protection Officer (DPO) who will undertake an investigation to determine the likelihood and severity of the risk to peoples' rights and freedoms. The Town Clerk and DPO If applicable, will report the breech to regulatory bodies, Council and the individuals concerned. They will also take

necessary steps to contain the breech and protect from any further breech. All data breeches will be recorded with justification for not reporting if this does not take place.

Freedom of Information Requests

Scope and Purpose

Under the Freedom of Information Act, Skegness Town Council has a duty to adopt and maintain a Publication Scheme describing:

- The classes of information it publishes;
- How and where such information is published (such as website, paper copy, etc); and
- Whether or not a charge is made for such information.

Other information is of course available from the Council by individual request, under the Freedom of Information Act 2000 and the Data Protection Act 1998, however as many requests are for routine information, this guide should assist the public in quickly and efficiently locating what they want.

If there is any information required that does not appear in this Publication Scheme or you have any comments or suggestions on how it can be improved, please contact the Town Clerk:

Obtaining Information

Much of the information listed in this Publication Scheme is supplied free of charge from our website. Where information is available only in paper format, this is also shown in the Scheme together with where any requests for such information should be directed and the cost.

Information not contained within the scheme and exemptions

Although the Freedom of Information Act 2000 creates a general right of access to information, it also sets out information that we do not have to make available for specific reasons, called exemptions. This is information that, if published, might prejudice the health, safety or security of the Council, our staff, systems, services or property.

The initial decision on whether to grant a request lies with the Clerk. Should he turn down a request, he must do so in writing, quoting any relevant exemptions. The applicant then has a right of appeal to a panel of Councillors convened for this purpose.

If after the appeal, the information is still not disclosed, the applicant can ask the Information Commissioner to review the decision.

Charges

Any copy and postage charges for publications are listed in the Publication Scheme.

If administration costs exceed £450, to enable a Freedom of Information request to be met, then the Council may charge the requestor for the administration costs in meeting that request.

Records Management

Is the set of activities required for systematically controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions.

Most Record Management activity will be governed on a day to day basis through procedure and is delegated to the Town Clerk to determine and will not be set out in detail within this policy.

General Principles:

All data, information and records will be kept for the minimum time permissible for the type of record as determined by legislation, good practice, the Town Clerk or as otherwise set by this policy. Copies of data shall be kept to an absolute minimum in accordance with good practice.

Paper Records
All paper based confidential or personal data/information shall be marked confidential or personal. Where this is being provided to Committee or Council for decision making purposes it shall be printed on “Pink Paper” and annotated with the recipient’s name. All paper based confidential/personal data/information shall be shredded prior to disposal. This may be carried out by a certified contractor or Council staff.

Electronic Records

Historically electronic data is more difficult to fully erase of as copies may have been made prior to this policy, that were not as fully controlled and so there is a potential risk to the Council, that personal information has been copied and stored electronically over the past 20 years.

Where electronic records contain personal or confidential data/information these for new records shall either:-

- Be stored in a named database or purpose built system that is password controlled; OR
- Be stored as a file where the file properties contains a tag identifying that the file contains personal or confidential data/information

To mitigate historic risk prior, wherever possible electronic data/information will be identified and either moved into the controlled systems or permanently deleted.

Retention Periods

The table below sets out the minimum retention periods for certain classes of records. Where there is an investigation, claim or other litigation process, all related record disposal will be suspended until the issue is settled. Where an item is not covered, the Town Clerk shall determine the minimum retention period.

Where an item falls into more than one class of record, the longer minimum retention period shall apply.

CLASS OF RECORD	**RETENTION PERIOD**
Accounting records	7 years after completion of audit
Allotment Tenancy Agreements and Financial Records	7 years
Annual returns	Indefinite
Bank statements and reconciliations	7 Years
Budget statements	2 Years
Burial records	Indefinite
Cemetery records	100 years
Contracts or agreements	7 years after expiry
Deeds	2 years after expiry
Electoral register	2 years
Financial transactions	7 years
Health and Safety Records	7 years
HR records (including payroll)	7 years
Licenses and permits	2 years after expiry
Minutes of Council and Committee Meetings	Indefinite
Pension records	Indefinite
Policies and strategies	Indefinite
Recruitment records	Upto 6 months

VAT and tax records	7 years

IMPLEMENTATION

ROLES AND RESPONSIBILITIES

All employees and Councillors will be responsible for:

- making sure you have read and understood the Information Security Policy and considered this in conjunction with the ICT Acceptable Use Policy;
- meeting the standards set out in this Policy and any associated guidance which may be published on the intranet from time to time;
- making sure that any Council ICT equipment that you take outside the work place including but not limited to laptops, mobile phones, iPads, are kept secure;
- reporting to the Council actual or potential breaches of the Council's ICT security and/or loss of confidential/personal data;
- returning any Council ICT equipment to the Council when you leave the Council.

If you use non Council issued equipment to access Council systems, these must only be "cloud based" applications where no data is stored or processed locally and the device is simply acting as a terminal. Should you download or process data or information locally on a non-Council device you will not be covered by the Council's Data Protection Registration and you may be breaking the law.

MONITORING

The policy will be monitored in the following ways:

MONITORING ACTIVITY	WHO IS RESPONSIBLE
Checking staff understanding of policy	Town Clerk
Annual check of compliance	Town Clerk/Deputy Town Clerk/DPO
Day to day compliance	All staff
Monitoring of risks	Management Committee
Day to day compliance	All staff
Information gathered by Council Members meets GDPR	Council Members
Managing FOI requests	Town Clerk/Deputy Town Clerk
Data Protection Requests/Complaints	Town Clerk/Deputy Town Clerk
Appeals	Committee established for this purpose

POLICY CONSULTATION

This policy will be published on the Council's web site.

POLICY APPROVAL

Approved by Council 16th December 2020

POLICY REVIEW DATE

December 2022

RELATED POLICIES & STRATEGIES

Information and Communications Technology (ICT) Acceptable Use Policy
Body Worn Cameras Policy
General Privacy Notice
Employee Privacy Notice