Louth Town Council

The Sessions House, Eastgate,
Louth, Lincolnshire, LN11 9AJ

01507 355895
clerk@louthtowncouncil.gov.uk
Town Clerk: Mrs. L. Phillips

CEMETERY PRIVACY NOTICE

When you purchase the Exclusive Right to a single or joint cemetery plot, arrange an interment or request permission for a memorial:

The information you provide (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible to contact you and to respond to your correspondence, provide information, send invoices and receipts relating to your burial plot/s. Your personal information will not be shared with any third party without your prior consent unless it is in relation to the grave, for example a Funeral Director or Memorial Mason).

The Councils Right to Process Information

GDPR Article 6 (1) (a) (b) and (c)

Processing is with consent of the data subject, or
Processing is necessary for compliance with a legal obligation, or
Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

Information Security

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

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

Your Rights

Access to Information

You have the right to request access to the information we have on you. You can do this by contacting the Data Control Officer: clerk@louthtowncouncil.gov.uk

Information Correction

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: clerk@louthtowncouncil.gov.uk

Information Deletion

If you wish Louth Town Council to delete the information about you, please contact: clerk@louthtowncouncil.gov.uk

Please note: Louth Town Council has a legal obligation to retain the personal details of owners of Exclusive Rights and Registrar consent for burial. This also includes cemetery information detailing the names of those buried or to be buried in the future within its burial grounds.

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact clerk@louthtowncouncil.gov.uk

Rights Related to Automated Decision Making and Profiling

Louth Town Council does not use automated decision making or profiling of personal data.

To Sum Up

In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell or pass your data to third parties (unless it is to a Funeral Director or Memorial Mason in relation to a grave). We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We constantly review our Privacy Policies to keep them up to date in protecting your data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to Louth Town Council Data Control Officer: clerk@louthtowncouncil.gov.uk and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Louth Town Council
The Sessions House, Eastgate,
Louth, Lincolnshire, LN11 9AJ

01507 355895
clerk@louthtowncouncil.gov.uk
Town Clerk: Mrs. L. Phillips

EMAIL CONTACT PRIVACY NOTICE

When you contact us

The information you provide (personal information such as name, address, email address, phone number, organisation) will be processed and stored so that it is possible to contact you and respond to your correspondence, provide information and/or access our facilities and services. Your personal information will be not shared or provided to any other third party.

The Councils Right to Process Information

GDPR Article 6 (1) (a) (b) and (e)

Processing is with consent of the data subject
or
Processing is necessary for compliance with a legal obligation
or
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Information Security

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

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

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Your Rights
Access to Information

You have the right to request access to the information we have on you. You can do this by contacting our Data Control Officer: Mrs. L. Phillips at The Sessions House, Eastgate, Louth LN11 9AJ or email: clerk@louthtowncouncil.gov.uk

Information Correction

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: clerk@louthtowncouncil.gov.uk

Information Deletion

If you wish Louth Town Council to delete the information about you please contact: clerk@louthtowncouncil.gov.uk

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact clerk@louthtowncouncil.gov.uk

Rights Related to Automated Decision Making and Profiling

Louth Town Council does not use automated decision making or profiling of individual personal data.

To Sum Up

In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell or pass your data to third parties. We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We constantly review our Privacy Policies to keep them up to date in protecting your data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to Louth Town Council Data Information Officer: clerk@louthtowncouncil.gov.uk and/or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

Louth Town Council
The Sessions House, Eastgate,
Louth, Lincolnshire, LN11 9AJ

01507 355895
clerk@louthtowncouncil.gov.uk
Town Clerk: Mrs. L. Phillips

GENERAL PRIVACY NOTICE

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by the Louth Town Council which is the data controller for your data.

Other data controllers the council works with:

- Other local authorities
- Community groups
- Charities
- Other not for profit entities
- Contractors

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

The council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;

- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email or telephone;
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.
- Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1) ***The right to access personal data we hold on you***

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.

- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) ***The right to correct and update the personal data we hold on you***

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) ***The right to have your personal data erased***

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) ***The right to object to processing of your personal data or to restrict it to certain purposes only***

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) ***The right to data portability***

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) ***The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

*7) **The right to lodge a complaint with the Information Commissioner's Office.***

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on www.louthtowncouncil.gov.uk This Notice was last updated in June 2019.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:
The Data Control Officer, Louth Town Council, The Sessions House, Eastgate, Louth, LN11 9AJ.
Email: clerk@louthtowncouncil.gov.uk

Louth Town Council
The Sessions House, Eastgate,
Louth, Lincolnshire, LN11 9AJ

01507 355895
clerk@louthtowncouncil.gov.uk
Town Clerk: Mrs. L. Phillips

PRIVACY NOTICE
FOR STAFF*, COUNCILLORS AND ROLE HOLDERS**

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis

**Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former Councillors. This also includes applicants or candidates for any of these roles.

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Louth Town Council which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.

- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases, photographs, video.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes:

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.

- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer Councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

- We may process sensitive personal data relating to staff, Councillors and role holders including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.

- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions, or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. ***The right to object to processing of your personal data or to restrict it to certain purposes only***

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. ***The right to data portability***

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. ***The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. ***The right to lodge a complaint with the Information Commissioner's Office.***

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on www.louthtowncouncil.gov.uk. This Notice was last updated in June 2019.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:
The Data Controller, Louth Town Council,The Sessions House, Eastgate, Louth, LN11 9AJ or email:clerk@louthtowncouncil.gov.uk.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Louth Town Council

DATA PROTECTION POLICY

Introduction

Louth Town Council needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on our work. This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this under the Data Protection Act 1998.

The following list of definitions of the technical terms we have used is intended to aid understanding of this policy.

Data Controller – The person who (either alone or with others) decides what personal information Louth Town Council will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

The Town Clerk – The person(s) responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998

Data Subject/Service User – The individual whose personal information is being held or processed by Louth Town Council (for example: a client, an employee, a supporter)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing* of personal information* about her/him. Explicit consent is needed for processing sensitive* data

* See definition

Notification – Notifying the Information Commissioner about the data processing activities of Louth Town Council as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Louth Town Council.

Sensitive data – means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership

- Physical or mental health
- Sexual life
- Criminal record
- Criminal proceedings relating to a data subject's offences

Data Controller

Louth Town Council is the Data Controller under the Act, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Disclosure

Louth Town Council may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Louth Town Council to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

Louth Town Council regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Louth Town Council intends to ensure that personal information is treated lawfully and correctly.

To this end, Louth Town Council will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)

4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Louth Town Council will, through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information),
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information.

Data collection

Informed consent

Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data

- and then gives their consent.

Louth Town Council will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Louth Town Council will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is Louth Town Council's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data access and accuracy

All Data Subjects have the right to access the information Louth Town Council holds about them Louth Town Council will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, Louth Town Council will ensure that:

- The Town Clerk has the specific responsibility for ensuring compliance with Data Protection,
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
- Everyone processing personal information is appropriately trained to do so,
- Everyone processing personal information is appropriately supervised,
- Anybody wanting to make enquiries about handling personal information knows what to do,
- It deals promptly and courteously with any enquiries about handling personal information,
- It describes clearly how it handles personal information,

- It will regularly review and audit the ways it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Louth Town Clerk.

Louth Town Council

INFORMATION SECURITY INCIDENT POLICY

Contents

Document Control

Organisation	
Title	
Creator	
Source	
Approvals	
Distribution	
Filename	
Owner	
Subject	
Protective Marking	
Review date	

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description

1 Purpose

1.1 This document defines an Information Security Incident and the procedure to report an incident

2 Scope

2.1 This document applies to all Councillors, Committees, Departments Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Louth Town Council purposes.

3 Definition

3.1 An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it, or data is at risk from corruption.

4 An Information Security Incident includes:

- The loss or theft of data or information
- The transfer of data or information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent
- Unwanted disruption or denial of service to a system
- The unauthorised use of a system for the processing or storage of data by any person.

5 When to report

5.1 All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported as soon as they happen.

6 Action on becoming aware of the incident

6.1 Follow the information security procedure, according to the type of incident.

7 How to report

7.1 The Data Control Officer must be contacted by email or in writing using the prescribed form. They will log the incident and forward it on to the relevant departments.

7.2 The Data Control Officer will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident
- The type of data or information involved
- Whether the loss of the data puts any person or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of data or equipment affected

- Type and circumstances of the incident.

7.3 Your line manager must also be informed to enable them to investigate and confirm that the details represent a valid security incident as defined above. The outcomes of these actions are to be reported to the Data Control Officer for inclusion in the incident details for investigation.

8 What to Report

8.1 All Information Security Incidents must be reported.

9 Examples of Information Security / Misuse Incident Protocols

9.1 Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

9.2 Malicious Incident

- Computer infected by a Virus or other malware, (for example spyware or adware)
- An unauthorised person changing data
- Receiving and forwarding chain letters – Including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Social engineering - Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).
- Unauthorised disclosure of information electronically, in paper form or verbally.
- Falsification of records, Inappropriate destruction of records
- Denial of Service, for example
- Damage or interruption to Louth Town Council equipment or services caused deliberately e.g. computer vandalism
- Connecting non-council equipment to the council network
- Unauthorised Information access or use
- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Printing or copying confidential information and not storing it correctly or confidentially.

9.3 Access Violation

- Disclosure of logins to unauthorised people
- Disclosure of passwords to unauthorised people e.g. writing down your password and leaving it on display
- Accessing systems using someone else's authorisation e.g. someone else's user id and password
- Inappropriately sharing security devices such as access tokens
- Other compromise of user identity e.g. access to network or specific system by unauthorised person
- Allowing Unauthorised Physical access to secure premises e.g. server room, scanning facility, dept area.

9.4 Environmental

- Loss of integrity of the data within systems and transferred between systems
- Damage caused by natural disasters e.g. fire, burst pipes, lighting etc
- Deterioration of paper records
- Deterioration of backup tapes

- Introduction of unauthorised or untested software
- Information leakage due to software errors.

9.5 Inappropriate use

- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Personal use of services and equipment in work time
- Using unlicensed Software
- Misuse of facilities, e.g. phoning premium line numbers.

9.6 Theft / loss Incident

- Theft / loss of data – written or electronically held
- Theft / loss of any Louth Town Council equipment including computers, monitors, mobile phones, Blackberries, Memory sticks, CDs.

9.7 Accidental Incident

- Sending an email containing sensitive information to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature, e.g. containing pornographic, obscene, racist, sexist, grossly offensive or violent material
- Receiving unsolicited mail which requires you to enter personal data.

9.8 Mis-keying

- Receiving unauthorised information
- Sending information to wrong recipient.

10 Escalation

10.1 Serious incidents will be escalated via the national WARP scheme if determined to be of national value.

Louth Town Council

REMOVABLE MEDIA POLICY

Contents

Document Control

Organisation	
Title	
Creator	
Source	
Approvals	
Distribution	
Filename	
Owner	
Subject	
Protective Marking	
Review date	

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description

1 Purpose

1.1 This policy supports the controlled storage and transfer of information by Councillors of Louth Town Council and all employees, temporary staff and agents (contractors, consultants and others working on behalf of the Council) who have access to and use of computing equipment that is owned or leased by Louth Town Council.

1.2 Information is used throughout the Authority and is sometimes shared with external organisations and applicants. The use of removable media may result in the loss of the ability to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of the Authority and may result in financial loss and an inability to provide services to the public.

1.3 It is therefore essential for the continued operation of the Authority that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Authority's needs.

1.4 The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:

- 1.4.1 Enabling the correct data to be made available where it is required
- 1.4.2 Maintaining the integrity of the data
- 1.4.3 Preventing unintended consequences to the stability of the computer network
- 1.4.4 Building confidence and trust in data that is being shared between systems
- 1.4.5 Maintaining high standards of care towards data and information about individual citizens, staff or information that is exempt from disclosure
- 1.4.6 Compliance with legislation, policies or good practice requirements

2 Scope

2.1 This policy sets out the principles that will be adopted by the Council in order for material to be safely stored on removable media so that the risk of loss or corruption to work data is low.

2.2 Removable media includes but is not limited to: USB memory sticks, memory cards, portable memory devices, CD / DVDs, diskettes and any other device that transfers data between systems, or stores electronic data separately from email or other applications.

2.3 Any person who intends to store Council data on removable media must abide by this Policy. This requirement devolves to Councillors, employees and agents of the Council, who may be held personally liable for any breach of the requirements of this policy.

2.4 Failure to comply with this policy could result in disciplinary action.

3 Advice and Assistance

3.1 The Data Control Officer and Clerk will ensure that everyone that is authorised to access the Authority's information systems is aware of their obligations arising from this policy.

3.2 The Data Control Officer and Clerk should be consulted over any hardware or system issues. The training section should be approached for advice and guidance on using software packages.

3.3 Should this policy appear to conflict with any other approved Council policy, then contact the Data Control Officer and Clerk for guidance.

4 Responsibilities

4.1 Chief Officers are responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Council business.

4.2 Users of removable media must have adequate Records Management / Information Security training so that relevant policies are implemented.

5 Incident Management

5.1 It is the duty of all employees and agents of the Council to not allow storage media to be compromised in any way whilst in their care or under their control. There must be immediate reporting of any misuse or irresponsible actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security to the Data Control Officer and Clerk.

5.2 It is the duty of all Councillors to report any actual or suspected breaches in information security to the Town Clerk.

6 Data Administration

6.1 Removable media should not be the only place where data created or obtained for work purposes is held, as data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up.

6.2 Where removable media is used to transfer material between systems then copies of the data should also remain on the source system or computer, until the data is successfully transferred to another computer or system.

6.3 Where there is a business requirement to distribute information to third parties, then removable media must only be used when the file cannot be sent or is too large to be sent by email or other secure electronic means.

6.4 Transferring material to removable media is a snapshot of the data at the time it was saved to the media. Adequate labelling must be undertaken so as to easily identify the version of the data, as well as its content.

6.5 Files must be deleted from removable media, or the removable media destroyed, when the operational use of the material has been completed. The Council's retention and disposition schedule must be implemented by Councillors, employees, contractors and agents for all removable media.

7 Security

7.1 All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption of the business asset. Due to their small size there is a high risk of the removable media being mislaid lost or damaged, therefore special care is required to physically protect the device and the data. Anyone using removable media to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

7.2 Virus Infections must be prevented from damaging the authority's network and computers. Virus and malware checking software approved by the Data Control Officer and Clerk must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by the virus checking software, before the media is loaded on to the receiving machine.

7.3 Any memory stick used in connection with Council equipment or to store Council material should usually be Council owned and be on the Louth Town Council approved list. However work related data from external sources can be transferred to the Council network using memory sticks that are from trusted sources and have been checked using current anti-virus software.

7.4 The Council will not provide support or administrator access for any non-council memory stick.

8 Use of removable media

8.1 Care must be taken over what data or information is transferred onto removable media. Only the data that is authorised and necessary to be transferred should be saved on to the device.

8.2 Material that is classified as RESTRICTED or higher must not be stored on removable media at any time.

8.3 Council material belongs to the Council and any equipment on which it is held should be under the control of the Council and not available to be used for other purposes that may compromise the data.

8.4 All data transferred to removable media should be in accordance with an agreed process established by the Directorate so that material can be traced.

8.5 The person arranging the transfer of data must be authorised to make use of, or process that particular data.

8.6 Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.

8.7 Encryption must be applied to the data file unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage. If encryption is not available then password control must be applied if removable media must be used for the business purpose.

9 Faulty or Unneeded Storage Devices

9.1 Damaged or faulty media must not be used. The Data Control Officer and Clerk must be consulted over any damaged equipment, peripherals or media.

9.2 All unneeded or faulty storage devices must be sent to the Data Control Officer and Clerk who will securely remove the data before reallocating or disposing of the device.

10 Requests to suspend this policy

10.1 This Policy is designed to protect Council business data and to accommodate the needs of users. However, should aspects of this policy interfere with a valid business requirement; an application can be made to the Data Control Officer and Clerk for an amendment to this policy. An outline risk assessment should be submitted with the application.

11 Breach procedures

11.1 Users who do not adhere to this policy will be dealt with through the Council's disciplinary process.

11.3 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

11.4 Where the public have access to the Louth Town Council system, that access will be withdrawn if there is an actual or likely breach of information security, until adequate controls are in place.

12 Review and Revision

12.1 This policy will be reviewed annually by the Data Control Officer and Clerk and revised according to developments in legislation, guidance, accepted good practice and operational use.

13 Key Messages for Staff

13.1 Data and information are valuable and must be protected.

13.2 Do not use removable media for material that is marked 'restricted' or above.

13.3 Only transfer data onto removable media, if you have the authority to do so.

13.4 All transfer arrangements carry a risk to the data.

13.5 Run the virus checking programme on the removable media each time it is connected to a computer.

13.6 Only use approved products for Council data.

13.7 Activate encryption on removable media wherever it is available and password protection if not available

13.8 Data should be available for automatic back up and not solely saved to removable media.

13.9 Delete files from removable media, or destroy the media, after the material has been used for its purpose.

13.10 Ask your manager if you are unsure.

Louth Town Council

RETENTION OF DOCUMENTS AND RECORDS POLICY

This policy details the minimum retention time required for Council documents before disposal in order for the council to comply with the Freedom of Information Act 2000 Publication Scheme. Where variable times are indicated the Council will review storage after the minimum period has elapsed. This document has been compiled using NALC Legal Topic Note 40.

DOCUMENT	MINIMUM PERIOD	REASON
Minute Books	Indefinite	Archive
Scale of fees and charges	6 years	Management
Receipt and payment account(s)	Indefinite	Archive
Receipt books of all kinds	6 years	VAT
Bank statements, including deposit/savings accounts	Last completed audit year	Audit
Bank paying-in books	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit
Quotations and tenders	6 years	Limitation Act 1980 (as amended)
Paid invoices	6 years	VAT
Paid cheques	6 years	Limitation act 1980 (as amended)
VAT records	6 years generally but 20 years for VAT on rents	VAT
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)
Wages books	12 years	Superannuation
Insurance policies	While valid	Management
Certificates for Insurance against liability for employees	40 years from date of which insurance commenced or was renewed	The Employer's Liability (Compulsory Insurance) Regulations 1998 (SI. 2753), Management
Investments	Indefinite	Audit, Management
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)
Re: Halls, Centre, Recreation Grounds		
• Application to hire • Lettings diaries • Copies of bills to hire • Record of tickets issued	6 years	VAT
Re: Allotments		
• Register and plans	Indefinite	Audit, Management
Re: Burial Grounds		
• Register of fees collected • Register of burials • Register of purchased graves • Register/plan of grave spaces • Register of memorials • Applications for interment • Applications for right to erect memorials • Disposal Certificates • Copy certificates of grant of exclusive right of burial	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI. 204)

Louth Town Council

SECURE DISPOSAL OF INFORMATION POLICY

Confidential electronic and paper information must be disposed of securely to minimise the risk of unwanted disclosure. Staff and Councillors must be sure to handle information securely. Achieving and demonstrating good standards of information handling is particularly important. Confidential information is information which if improperly disclosed or lost could cause harm or distress. This includes personal data as defined by the Data Protection act, i.e. information about a living individual from which that individual could be identified, and other valuable or sensitive information not in the public domain.

Procedures

Appropriate procedures must be followed when disposing of information, whether it is in paper or electronic form, to minimise the risk of unwanted disclosure.

Precautions must be taken when control of a device that may have information stored locally is to be reassigned to someone else. (Such devices include: computers, mobile phones, USB drives, cameras, rewritable CDs/DVDs etc.)

When devices that store confidential information are to be repaired, then that information should first be removed. However, if removal of the information prior to repair is not possible the work should be carried out by a company subject to a suitable agreement.

In general, locally installed licensed software should be removed from IT equipment before disposal or transfer of control. Not doing so may breach the terms of the licence.

Disposing of paper information

Dispose of unwanted paper documents that do not contain any confidential information by recycling.

Where documents contain confidential information, assess whether the disclosure of the information could cause harm. If so, or if you are uncertain, place the documents in a shredding bag and store the bag securely pending shredding.

Disposing of electronic information

In general, Councillors and staff are advised not to save any documents relating to Council business on their devices. Copies of 'live' documents should be available on the Council's website, for perusal.

However, Councillors and staff should ensure that locally stored confidential information is removed as appropriate before a device is reassigned to another person. This should be done routinely using a secure file or drive level deletion tool – see below.

In the case of Louth Town Council owned Councillor email accounts, upon a Councillor ceasing service with Louth Town Council, control of these will be taken back by the Data Control Officer who will ensure that data is deleted, as required, before reallocation of the email account.

Secure data deletion tools

The standard method of deleting a data file, on many types of system, may leave its contents recoverable. This is helpful if a mistake has been made, however, it is insecure if the intention is to prevent anyone else being able to "un-delete" and read the file. (Tools for recovering files deleted in the standard way are available for various systems.)

Equipment hard drives can be "securely wiped", such that the data is made unrecoverable.

However, whilst some Councillors and staff may feel confident to obtain / use secure data deletion tools others needing to ensure that confidential data has been deleted are advised to seek assistance from the Data Control Officer.

Louth Town Council

SUBJECT ACCESS REQUESTS POLICY

All Subject Access Requests (SAR's) must be received in writing and should be forwarded immediately to the Data Control Officer and Clerk.

1) Upon receipt of a SAR

The Data Control Officer will:

a) Verify whether Louth Town Council is the controller of the data subject's personal data. If Louth Town Council is not the controller, but merely a processor, Louth Town Council will inform the data subject and refer them to the actual controller.
b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
c) Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.
d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.
e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
f) Verify whether Louth Town Council process the data requested. If it does not process any data, inform the data subject accordingly.
g) At all times make sure the internal SAR policy is followed and progress can be monitored.
h) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
i) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2) Responding to a SAR

The Data Control Officer will:

a) Respond to a SAR within one month after receipt of the request.
b) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;
c) If the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
d) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.
e) If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:
    i) the purposes of the processing;
    ii) the categories of personal data concerned;
    iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses;
    iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
    v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    vi) the right to lodge a complaint with the **Information Commissioners Office** ("ICO");
    vii) if the data has not been collected from the data subject: the source of such data;
    viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
    ix) Provide a copy of the personal data undergoing processing.

Louth Town Council

COMPLAINTS PROCEDURE

To determine whether a complaint procedure is appropriate:

1) It will not be appropriate to deal with all complaints from members of the public under a complaints procedure. The Council will need to refer or use procedures / bodies in respect of the following types of complaint:

Individual member's conduct alleged to breach the Code of Conduct adopted by the Council	*The relevant principal authority Monitoring Officer should be contacted – East Lindsey District Council has responsibility for such matters*
Alleged financial irregularity	*Local electors have a statutory right to object to a Council's audit of accounts (Audit Commission Act 1998 s.16)*
Alleged criminal activity	*The Police*

2) A member of the public may also consider a criticism about a service (e.g. an untidy park area or unclean public toilet) or a fee (e.g. the level of charge for an allotment) to be a complaint, but these do not fall within the formal complaints procedure unless the Council has acted improperly and should be treated as normal service requests.

3) It is to be noted that staff members are not responsible for any works or maintenance carried out by any Town Council appointed contractor(s); such complaints must be made in writing to the Council. Person(s) who make such complaints 'personal' against staff members may be subject to restrictions within other Town Council Policies.

Before the meeting

1. Any complaint about the Council's procedures or administration should be made in writing to the Clerk to the Council at The Sessions House, Eastgate, Louth, LN11 9AJ

2. If the complainant does not wish to make the complaint via the Clerk to the Council, it should be marked confidential and addressed to the Chairman (Mayor) of the Council.

3. The Clerk to the Council/Chairman will acknowledge receipt of the complaint and advise when the matter will be considered by either the Council or a nominated Committee working on behalf of the Council.

4. Please be aware that any complaint will be treated as confidential, and that the council is obliged to comply with its duties under the Data Protection Act 1998 at all times to safeguard against the unlawful disclosure of personal data.

5. The complainant will be invited to attend the meeting at which the complaint will be considered, and be offered the opportunity to be accompanied by a representative, if required.

6. Seven clear working days prior to the meeting, the complainant is required to provide the Council with copies of any documentation or other items on which the complaint is based.

7. The Council will provide the complainant with copies of any documentation upon which it wishes to rely at the meeting and shall do so promptly, allowing the opportunity to read all material in good time for the meeting.

Louth Town Council

COMPLAINTS PROCEDURE

At the meeting

1. The council shall exclude the public and press whilst discussion of the matter takes place. Any decision on a complaint shall subsequently be announced at a meeting in public, whilst taking into account any duties to safeguard personal data as under (4) above.

2. The Chairman will introduce everyone at the meeting, and explain the procedure to be followed.

3. The complainant will be asked to outline the grounds for the complaint, and thereafter, questions may be asked by (i) the Clerk and (ii) members of the Council.

4. The Clerk to the Council will then have an opportunity to explain the Council's position and questions may be asked by (i) the complainant and then (ii) members.

5. The complainant will be offered the opportunity to summarise their position.

6. The Clerk will be offered the opportunity to summarise the position on behalf of the Council.

7. The Clerk and complainant will both be asked to leave the room whilst members decide whether or not the grounds for the complaint have been made. If a point of clarification is necessary, both parties shall be invited back.

8. The complainant will be given the opportunity to await the outcome but if a decision is unlikely to be finalised quickly, will be advised when a decision is likely to be made and communicated to them.

After the meeting

1. Any decision will be confirmed to the complainant within seven working days, together with details of any further action to be taken.

Louth Town Council

POLICY ON HANDLING OF FREEDOM OF INFORMATION REQUESTS

- Louth Town Council has produced and publicised a Publication Scheme, which makes it clear what information can already be accessed. The Publication Scheme outlines any charges which may be made in supplying any information.
- Any additional information which is not part of the Publication Scheme can be requested under the Freedom of Information Act 2000.
- A request for information must be made by letter or e-mail and should be sent to the Clerk to the Council. The request must include a contact name, an address for correspondence and state clearly what information is required.
- Responsibility for dealing with all requests for information has been delegated to the Clerk to the Council.
- The first step will be to identify whether the requested data is held by the council. If not, the applicant will be notified accordingly.
- If information is held, and is not subject to any exemption, it will normally be supplied within 20 working days unless there is a fee to pay, or further clarification must be sought.
- If the request for information is unclear, the Clerk to the Council will contact the applicant to clarify what data is being sought. If clarification of a request is needed, the 20 working day period will commence on receipt of the additional information.
- If the information is not held by the Council, but the Council is aware of another public body which may hold the information, the request will either be forwarded to the third party concerned, or the applicant will be given details of which public authority is believed to hold the information.
- Where information cannot be provided, a refusal notice will be issued explaining which exemption applies, and advising of any right to appeal, if applicable.
- Where information is subject to a 'qualified exemption' under the FOI Act, there may be an extension to the 20 day period whilst further consideration is given to applying the public interest test, to determine whether any information should be withheld or disclosed.
- Where any complaint is received about the processing of any request for information, this will be referred on to full Council for attention.
- Where any correspondence is received from the Information Commissioner's Office in relation to any Freedom of Information matter, this will be referred on to full Council for attention.

Louth Town Council

MEDIA POLICY

Aims: Louth Town Council aims to build and maintain a positive reputation and will have a proactive approach to dealing with the media with enquiries being dealt with, wherever possible, within two working days. This approach will ensure an open and transparent approach which is helpful to the media and is positive and honest.

Objectives: 1) To improve residents' understanding of the work of the Council and to provide public information. 2) To enhance the reputation of Louth Town Council by promoting and celebrating success and the achievements of the Council and its partners. 3) To ensure a co-ordinated response from a single point of communication, the Town Clerk. 4) Reduce the risk of negative publicity resulting from non-response to enquiries. 5) To defend the Council from unfounded criticism by ensuring the public are properly informed of all relevant facts. 6) Adhere to the Code of Recommended Practice on Local Authority publicity.

Roles and Responsibilities: The Council's policy is to deal with all media enquiries centrally through the town Clerk. This will ensure that a consistent message is given. Any statements given must not be party political.

Councillors: All elected members should be sensitive to the fact that they are perceived to be speaking on behalf of the Council. If they are writing or saying something that is not in accordance with Council Policy they should make it clear that it is their view and not the Council's. The Town Clerk should be informed if Councillors do make a statement so it does not come as a surprise.

Privacy: All matters discussed in private must remain confidential and should not be leaked in any form to the media. (Notes taken when the Council is in Committee must be handed in and mobile phones must be switched off). Disciplinary action will be considered if Councillors are found to have "leaked" any confidential information.

Radio and Television Interviews: All elected members should be sensitive to the fact that they are perceived to be speaking on behalf of the Council. If they are saying something that is not in accordance with Council Policy they should make it clear that it is their view and not the Council's. Out of courtesy the Town Clerk should be informed of any radio or television interviews.

Management of Negative Publicity: It is important that this is done well and points adhered to. Inaccurate reporting in the media to be discussed by the Town Clerk and Mayor and Councillors invited to give their views where appropriate before a course of action is decided on.

Social Media: Councillors and staff should remember that all social media sites are a public forum and that they are personally responsible for the content published. No defamatory, derogatory or offensive comments should be posted on the internet about colleagues or matters which have come in front of the Council. Anyone acting in contravention of this protocol may be subject to misconduct and disciplinary action.

Equal Opportunities and Diversity: These must be respected and adhered to at all times, when dealing with any form of media. The Town Council shall not publish any material which in whole, or in part, appears to be designed to support a political party.

Embargoes: To be used where deemed necessary and, all press releases should carry the embargoed logo on the top sheet. The Town Clerk, the Mayor and Councillors will convene a meeting to decide on a course of action should any media break the Council's stated embargo.

Press Conferences: Can be convened in the event of a major incident or an emergency in the town. Any press conferences held need to be pre-planned so that individuals know they will speak and know what they will say. All press conferences should be run to an agreed framework.